

Contents

管理應用程式

概觀

應用程式管理概觀

快速入門

新增並指派應用程式

建立和指派應用程式防護原則

教學課程

保護受管理裝置上的電子郵件

保護未受管理裝置上的電子郵件

設定 Slack 以使用 Intune

概念

應用程式生命週期

應用程式防護原則與工作設定檔 (Android)

在沒有 Google Mobile Services 的情況下使用 Intune

MAM 常見問題集

操作指南

新增應用程式

新增應用程式概觀

受 Intune 保護的應用程式

市集應用程式

Android 市集應用程式

iOS 市集應用程式

Microsoft Store 應用程式

商務用 Microsoft Store 應用程式

受管理的 Google Play 應用程式

Microsoft 365 Suite

適用於 Windows 10 的 Microsoft 365 Apps

適用於 macOS 的 Microsoft 365 Apps

Android 企業版系統應用程式

Web 應用程式

內建應用程式

建置您的應用程式 (LOB)

Android LOB 應用程式

iOS LOB 應用程式

Windows LOB 應用程式

側載 Windows LOB 應用程式

macOS LOB 應用程式

macOS 應用程式管理

macOS 的 Intune 管理代理程式

新增 macOS DMG 應用程式

Win32 應用程式管理

Win32 應用程式管理概觀

準備 Win32 應用程式

新增 Win32 應用程式

Win32 應用程式取代

疑難排解 Win32 應用程式

Win32 應用程式 S 模式裝置

部署 Windows 更新套件

新增特定應用程式

公司入口網站應用程式 - Autopilot

公司入口網站應用程式 - 下載

公司入口網站應用程式 - macOS

適用於 Windows 10 的 Microsoft Edge

適用於 macOS 的 Microsoft Edge

Mac 版適用於端點的 Microsoft Defender

PowerShell 指令碼

macOS 殼層指令碼

指派應用程式

將應用程式指派給群組

包含和排除應用程式

部署 Windows 10/11 應用程式

將應用程式部署到政府環境

監視應用程式

探索到的應用程式

設定應用程式

應用程式設定原則

受 iOS 管理的裝置

受 Android 管理的裝置

受管理應用程式

使用 iOS 應用程式佈建設定檔

設定特定應用程式

設定受管理主畫面

設定公司入口網站

設定 Microsoft Launcher

設定 Microsoft Edge

設定 Office

設定 Outlook

設定 Microsoft Teams

設定 Android 版 Google Chrome

Android 企業版上的 VPN 和每個應用程式 VPN

大量購買的應用程式和書籍

大量購買概觀

大量購買 iOS 應用程式

商務用 Microsoft Store 應用程式

iOS 電子書

保護應用程式

選擇性抹除應用程式

使用應用程式防護原則

應用程式防護原則概觀

使用應用程式防護原則的資料保護架構

建立應用程式防護原則

一般設定

Android 設定

[iOS 設定](#)

[條件式啟動](#)

[資料傳輸例外狀況](#)

[驗證應用程式防護原則](#)

[應用程式防護原則交付](#)

[保護應用程式延伸模組](#)

[監視應用程式防護使用者狀態](#)

[為 WIP 應用程式防護原則做好準備](#)

[建立和指派 WIP 應用程式防護原則](#)

[管理 iOS 應用程式之間的資料傳輸](#)

[檢閱應用程式防護記錄](#)

[Office 應用程式的原則](#)

[疑難排解](#)

[協助使用者疑難排解問題](#)

[疑難排解應用程式安裝問題](#)

[應用程式安裝錯誤參考](#)

[疑難排解行動裝置應用程式管理](#)

[檢閱應用程式防護記錄](#)

[疑難排解應用程式防護原則部署](#)

[參考](#)

[使用 Intune App SDK 保護應用程式](#)

[開始使用 Intune App SDK](#)

[為應用程式防護準備 LOB 應用程式](#)

[適用於 iOS 的應用程式包裝工具](#)

[適用於 iOS 的 Intune App SDK](#)

[適用於 Android 的應用程式包裝工具](#)

[適用於 Android 的 Intune App SDK](#)

[適用於 Android 的 Intune App SDK 測試指南](#)

[Intune App SDK Xamarin Bindings](#)

什麼是應用程式管理Microsoft Intune？

2022/9/27 •

身為 IT 系統管理員，您可以使用Microsoft Intune來管理公司員工所使用的用戶端應用程式。這項功能是管理裝置及保護資料的補充功能。系統管理員的其中一個優先要務是確保使用者能夠存取執行工作所需的應用程式。這是一項具挑戰的目標，因為：

- 裝置平台和應用程式類型非常多樣。
- 您可能需要一併管理公司裝置和使用者個人裝置上的應用程式。
- 您必須確保網路和資料仍然安全。

此外，您可能會想要在未向 Intune 註冊的裝置上指派及管理 應用程式。

行動應用程式管理 (MAM) 基本概念

[Intune行動應用程式管理](#)是指Intune管理功能套件，可讓您為使用者發佈、推送、設定、保護、監視及更新行動應用程式。

MAM 可讓您管理和保護應用程式內的組織資料。許多生產力應用程式 (例如 Microsoft Office 應用程式) 都可由 Intune MAM 管理。請參閱可公開使用的 [Microsoft Intune 受保護應用程式](#)官方清單。

Intune MAM 支援兩種設定：

- **Intune MDM + MAM**：IT 系統管理員可以在Intune行動裝置管理 (MDM) 註冊的裝置上，使用 MAM 來管理應用程式。若要使用 MDM + MAM 管理應用程式，客戶應該在 [Microsoft 端點管理員系統管理中心使用Intune](#)。
- **使用 MAM 受控應用程式取消註冊的裝置**：IT 系統管理員可以在已取消註冊的裝置或向協力廠商 EMM 提供者註冊的裝置上，使用 MAM 管理應用程式中的資料和帳戶。若要使用 MAM 管理應用程式，客戶應該在[Microsoft 端點管理員系統管理中心使用Intune](#)。如需 BYOD 和 Microsoft EMS 的詳細資訊，請參閱使用[Microsoft Enterprise Mobility + Security \(EMS\) 啟用 BYOD 的技術決策](#)。

依平台的 Intune 應用程式管理功能

Intune 提供一系列功能，可協助您在您想要的裝置上，取得所需的應用程式。下表提供應用程式管理功能的摘要。

功能	ANDROID/ANDROID TABLET	IOS/IPADOS	MACOS	WINDOWS 10/11
新增應用程式並指派給裝置和使用者	是	是	是	是
將應用程式指派給未向 Intune 註冊的裝置	是	是	否	否
使用應用程式設定原則來控制應用程式的啟動行為	是	是	否	否
使用行動裝置應用程式布建原則來更新過期的應用程式	否	是	否	否
使用應用程式保護原則保護應用程式中的公司資料	是	是	否	否 ¹
只從已安裝的應用程式移除公司資料，(應用程式選擇性抹除)	是	是	否	是
監視應用程式指派	是	是	是	是
從 App Store 指派和追蹤大量採購的應用程式	否	否	否	是
在裝置上強制安裝應用程式 (需要) ²	是	是	是	是

	ANDROID/ANDROID TV	IOS/IPADOS	MACOS	WINDOWS 10/11
從可用安裝公司入口網站 (裝置上選擇性安裝)	是 ³	是	是	是
在 Web 連結 (安裝應用程式的快捷方式)	是 ⁴	是	是	是
內部 (企業營運) 應用程式	是 ⁵	是	是	是
來自市集的應用程式	是	是	否	是
更新應用程式	是	是	否	是

¹考慮使用[Microsoft Purview 資訊保護](#)和[Microsoft Purview 資料外洩防護](#)。Microsoft Purview 可簡化組態設定，並提供一組進階功能。

²僅適用於Intune所管理的裝置。

³Intune支援來自 Android Enterprise 裝置上受控 Google Play 商店的可用應用程式。

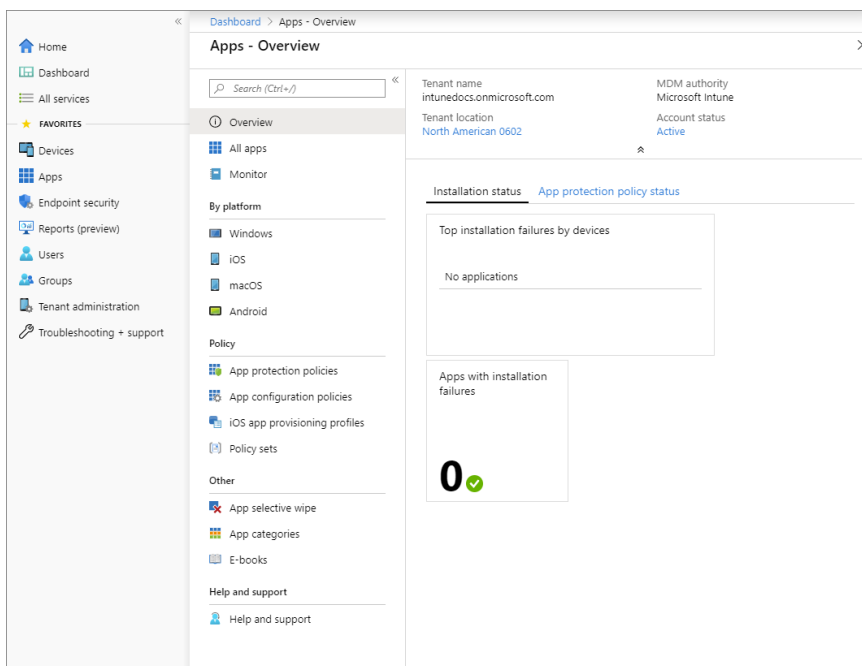
⁴Intune不提供將應用程式的快捷方式安裝為標準 Android Enterprise 裝置上的 Web 連結。不過，會為[多應用程式專用 Android 企業版裝置](#)提供網頁連結支援。

支援⁵個適用於 AE 的 LOB，但應用程式必須私下發布至 Managed Play。

快速入門

您可以在 **應用程式** 工作負載中找到大部分的應用程式相關資訊，您可以執行下列動作來存取此工作負載：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式]。



應用程式工作負載提供連結以存取一般應用程式資訊和功能。

[應用程式工作負載] 導覽功能表頂端提供常用的應用程式詳細資料：

- **概觀**：選取此選項可檢視租使用者名稱、MDM 授權單位、租使用者位置、帳戶狀態、應用程式安裝狀態和應用程式保護原則狀態。
- **所有應用程式**：選取此選項可顯示所有可用應用程式的清單。您可以從此頁面新增其他應用程式。此外，您可以查看每個應用程式的狀態，以及是否已指派每個應用程式。如需詳細資訊，請參閱 [新增應用程式](#) 和 [指派應用程式](#)。
- **監視應用程式**
 - **應用程式授權**：檢視、指派及監視從應用程式市集大量採購的應用程式。如需詳細資訊，請參閱 [iOS 大量採購方案 \(VPP\) 應用程式](#) 和 [商務用 Microsoft Store 大量採購的應用程式](#)。
 - **探索到的應用程式**：檢視由Intune指派或安裝在裝置上的應用程式。有關詳細資訊，請參閱 [Intune 發現的應用程式](#)。
 - **應用程式安裝狀態**：檢視您所建立應用程式指派的狀態。如需詳細資訊，請參閱 [使用 Microsoft Intune 監視應用程式資訊和指派](#)。
 - **應用程式防護狀態**：檢視您所選使用者的應用程式保護原則狀態。

- **依平臺**：選取這些平臺以依平臺檢視可用的應用程式。
 - Windows
 - iOS
 - macOS
 - Android
- **原則**：
 - **應用程式防護原則**：選取此選項可建立設定與應用程式的關聯，並協助保護其所使用的公司資料。例如，您可能限制應用程式與其他應用程式通訊的功能，或要求使用者輸入 PIN 以存取公司應用程式。如需詳細資訊，請參閱 [應用程式防護原則](#)。
 - **應用程式設定原則**：選取此選項可提供使用者執行應用程式時可能需要的設定。如需詳細資訊，請參閱 [應用程式設定原則](#)、[iOS 應用程式設定原則](#)，和 [Android 應用程式設定原則](#)。
 - **iOS 應用程式布建設定檔**：iOS 應用程式包含由憑證簽署的布建設定檔和程式碼。當憑證到期時，即無法再執行應用程式。Intune提供工具，讓您主動將新的布建設定檔原則指派給應用程式即將到期的裝置。如需詳細資訊，請參閱 [iOS 應用程式布建設定檔](#)。
 - **S 模式補充原則**：選取此選項可授權其他應用程式在受控 S 模式裝置上執行。如需詳細資訊，請參閱 [S 模式補充原則](#)。
 - **Office 應用程式的原則**：選取此選項可為連線到 Microsoft 365 服務的 Office 行動應用程式建立行動應用程式管理原則。您也可以為啟用混合式新式驗證的 iOS/iPadOS 和 Android 版 Outlook 建立 Intune 應用程式防護原則，以保護 Exchange 內部部署信箱的存取權。您必須符合使用 Office 應用程式原則的需求。如需對需求的詳細資訊，請參閱 [使用 Office 雲端原則服務的需求](#)。連線到內部部署 Exchange 或 SharePoint 服務的其他應用程式不支援應用程式防護原則。如需相關資訊，請參閱 [Microsoft 365 應用程式企業版的 Office 雲端原則服務概觀](#)。
 - **原則集合**：選取此選項可建立您已建立的應用程式、原則和其他管理物件的可指派集合。如需詳細資訊，請參閱 [原則集合](#)。
- **其他**：
 - **應用程式選擇性抹除**：選取此選項，只從選取的使用者裝置移除公司資料。如需詳細資訊，請參閱 [應用程式選擇性抹除](#)。
 - **應用程式類別**：新增、釘選和刪除應用程式類別名稱。
 - **電子書**：某些應用程式市集可讓您為想要在公司中使用的應用程式或書籍購買多個授權。如需詳細資訊，請參閱 [使用 Microsoft Intune 管理大量採購的應用程式和書籍](#)。
- **說明及支援**：疑難排解、要求支援或檢視Intune狀態。如需詳細資訊，請參閱 [疑難排解問題](#)。

嘗試互動式指南

使用[Microsoft 管理及保護行動和桌面應用程式端點管理員](#)互動式指南會逐步引導您完成 Microsoft 端點管理員系統管理中心，以示範如何管理在Intune中註冊的裝置、強制遵循原則，以及保護組織的資料。

<https://mslearn.cloudguides.com/guides/Manage%20and%20protect%20mobile%20and%20desktop%20applications%20with%20Microsoft%20Intune>

其他資訊

主控台內的下列專案提供應用程式相關功能：

- **商務用 Microsoft Store**：設定與商務用 Microsoft Store的整合。之後，您可以將購買的應用程式同步至 Intune、指派應用程式，以及追蹤您的授權使用量。如需詳細資訊，請參閱[商務用 Microsoft Store大量採購的應用程式](#)。
- **Windows 企業憑證**：套用或檢視程式碼簽署憑證的狀態，該憑證可用來將企業營運應用程式散發至受控 Windows 裝置。
- **Windows Symantec 憑證**：套用或檢視 Symantec 程式碼簽署憑證的狀態。
- **Windows 端載入金鑰**：新增 Windows 側載金鑰，可用來將應用程式直接安裝到裝置，而不是從 Windows 市集發佈和下載應用程式。如需詳細資訊，請參閱[側載 Windows 應用程式](#)。
- **Microsoft 端點Configuration Manager**：顯示Configuration Manager連接器的相關資訊，包括上次成功的同步處理時間和線上狀態。選取執行版本 2006 或更新版本的組態管理員階層，以顯示其他相關資訊。
- **Apple Business Manager 位置權杖**：套用並檢視您 iOS/iPadOS 大量購買的授權。如需詳細資訊，請參閱[如何使用 Microsoft Intune 管理透過 Apple Business Manager 購買的 iOS 和 macOS 應用程式](#)。
- **受控 Google Play**：受控 Google Play 是 Google 的企業應用程式市集，也是 Android Enterprise 應用程式的唯一來源。如需詳細資訊，請參閱[使用 Intune 將受管理的 Google Play 應用程式新增至 Android Enterprise 裝置](#)。
- **自訂**：自訂公司入口網站，為其提供公司商標。如需詳細資訊，請參閱[公司入口網站組態](#)。

如需應用程式的詳細資訊，請參閱[將應用程式新增至Microsoft Intune](#)。

後續步驟

- [將應用程式新增至 Microsoft Intune](#)

快速入門：新增和指派應用程式

2022/9/27 •

在本快速入門中，您將使用Intune來新增應用程式，並將應用程式指派給公司的員工。系統管理員的其中一個優先要務是確保使用者能夠存取執行工作所需的應用程式。

如果您沒有Intune訂用帳戶，請[註冊免費試用帳戶](#)。

先決條件

- 若要完成本快速入門，您必須 [建立使用者](#)、[建立群組](#)，以及 [註冊裝置](#)。

登入 Intune

以全域管理員或Intune服務系統管理員身分登入 Microsoft 端點管理員 系統管理中心。如果您已建立Intune試用版訂用帳戶，您使用 建立訂用帳戶的帳戶就是全域管理員。

將應用程式新增至 Intune

您可以包含應用程式，讓Intune可以管理應用程式的各個層面。

使用下列步驟將應用程式新增至 Intune：

- 登入 [Microsoft 端點管理員 系統管理中心](#)，選取 [應用程式 > 所有應用程式 > 新增]。
- 在 [應用程式類型] 下拉式方塊中，從 [Microsoft 365 Apps] 選取 [Windows 10**] 和 [更新** 版本]。
- 按一下 [選取]。[新增應用程式] 步驟隨即顯示。
- 確認 應用程式套件資訊 步驟中的預設詳細資料，然後按 [下一步]。
- 確認 [應用程式設定] 步驟中的預設設定，然後按 [下一步]。
- 選取應用程式的群組指派。如需詳細資訊，請 [參閱新增群組以組織使用者和裝置](#)。
- 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。檢閱您為應用程式輸入的值和設定。
- 當您完成時，按一下 [建立] 將應用程式新增至Intune。

將應用程式指派給群組

將應用程式新增至Microsoft Intune之後，您可以將應用程式指派給其他使用者或裝置群組。

NOTE

本快速入門是以本系列先前的快速入門為基礎。如需詳細資訊，請參閱本快速入門中的 [必要](#) 條件。

使用下列步驟將應用程式指派給群組：

- 在 [Intune] 中，選取 [所有應用程式 >]。
- 選取您要指派給群組的應用程式。
- 按一下 [內容]。按一下 [指派] 旁的 [編輯]。
- 按一下 [必要] 區段下的 [新增群組**]**。[選取群組] 窗格隨即顯示。
- 尋找您需要新增的群組，然後按一下窗格底部的 [選取]。
- 按一下 [檢視 + 儲存] > 以指派群組。****

您現在已將應用程式指派給其他群組。

在已註冊的裝置上安裝應用程式

終端使用者必須安裝並使用公司入口網站應用程式，才能安裝 Intune 所提供的應用程式。身為終端使用者的您，可以使用下列步驟來確認已註冊裝置的使用者可以使用該應用程式。

1. 登入已註冊Windows 10桌面裝置。

IMPORTANT

裝置必須[向Intune註冊](#)。此外，您必須使用您指派給應用程式的群組中所包含的帳戶來登入裝置。

2. 從 [開始] 功能表開啟 **Microsoft Store**。然後，尋找 **公司入口網站 應用程式** 並加以安裝。
3. 啟動 **公司入口網站 應用程式**。
4. 按一下您使用 Intune 新增的應用程式。在本快速入門中，您已新增 **Microsoft 365 Apps** 套件。

NOTE

如果您未成功將任何應用程式指派給Intune使用者，您會看到下列訊息：*您的 IT 系統管理員並未將任何應用程式提供給您。*

5. 按一下 [安裝]。

如果您的業務需求需要將公司入口網站應用程式指派給員工，您可以直接從Intune手動指派Windows 10 公司入口網站應用程式。如需詳細資訊，請[參閱使用 Microsoft Intune 手動新增Windows 10 公司入口網站應用程式](#)。

後續步驟

在本快速入門中，您已將應用程式新增至Intune、將應用程式指派給群組，以及在已註冊Windows 10桌面裝置上安裝應用程式。如需在Intune中管理應用程式的詳細資訊，請參閱[什麼是Microsoft Intune應用程式管理？](#)

若要繼續追蹤此 Intune 快速入門系列，請前往下一個快速入門。

[快速入門: 建立和指派應用程式保護原則](#)

快速入門：建立和指派應用程式保護原則

2022/9/27 •

在本快速入門中，您將使用Intune建立應用程式保護原則，並將應用程式保護原則指派給終端使用者裝置上的用戶端應用程式。Intune使用應用程式保護原則來確認您的應用程式符合組織的資料保護需求。

如果您沒有Intune訂閱帳戶，請[註冊免費試用帳戶](#)。

先決條件

- 若要完成本快速入門，您必須 [建立使用者](#)、[建立群組](#)、[註冊裝置](#)，以及 [新增和指派應用程式](#)。

登入 Intune

以[全域管理員](#)或Intune服務管理員身分登入Intune。如果您已建立Intune試用版訂閱帳戶，您使用 [建立訂閱帳戶](#)的帳戶就是全域管理員。

建立應用程式防護原則

使用下列步驟來建立應用程式防護原則：

- 在 [Intune](#)中，選取 [\[應用程式 > 應用程式防護原則 > 建立原則 > Windows 10\]](#)。
- 輸入下列詳細資料：
 - 名稱：*Windows 10內容保護*
 - 描述：*與此原則相關聯的使用者將無法在指派的應用程式與裝置上其他非受控應用程式之間剪下、複製或貼上任何內容。*
 - 註冊狀態：*使用註冊*
- 在 [\[受保護的應用程式\]](#) 底下，按一下 [\[新增\]](#)。[\[新增應用程式\]](#) 窗格隨即顯示。
- 選擇必須遵守此原則的應用程式，然後按一下 [\[確定\]](#)。
- 按 [\[下一步\]](#) 以顯示 [\[必要\]](#) 設定。
- 按一下 [\[允許覆寫\]](#) 以設定 Windows 資訊保護模式。選取此選項會封鎖企業資料離開受保護的應用程式。
- 按 [\[下一步\]](#) 以顯示 [\[進階\]](#) 設定。
- 按 [\[下一步\]](#) 以顯示 [\[指派\]](#)。
- 按一下 [\[選取要包含的群組\]](#)、按一下群組，然後按一下 [\[選取\]](#)。
- 按 [\[下一步\]](#) 以顯示 [\[檢閱 + 建立\]](#) 步驟。
- 按一下 [\[建立\]](#) 以建立您的原則。

您現在會在Intune中看到應用程式保護原則。

NOTE

應用程式防護原則只能套用至包含使用者的群組，不能套用至包含裝置的群組。

後續步驟

在本快速入門中，您已建立並指派應用程式保護原則。已指派此原則的應用程式使用者將無法在指派的應用程式與裝置上的其他非受控應用程式之間剪下、複製或貼上任何內容。這種類型的保護可協助保護貴組織的資料。如需Intune中應用程式保護原則的詳細資訊，請參閱[什麼是應用程式保護原則？](#)

若要繼續追蹤此 Intune 快速入門系列，請前往下一個快速入門。

[快速入門: 建立和指派自訂角色](#)

教學課程：保護受管理裝置上 Exchange Online 電子郵件

2022/9/27 •

瞭解如何搭配條件式存取使用裝置合規性原則，以確保 iOS 裝置只有在受 Intune 管理並使用已核准的電子郵件應用程式時，才能存取 Exchange Online 電子郵件。

在本教學課程中，您將瞭解如何：

- 建立 Intune iOS 裝置合規性政策，以設定裝置必須符合才能視為符合規範的條件。
- 建立 Azure Active Directory (Azure AD) 條件式存取原則，要求 iOS 裝置註冊 Intune、遵守 Intune 原則，以及使用核准的 Outlook 行動應用程式來存取 Exchange Online 電子郵件。

如果您沒有 Intune 訂用帳戶，請[註冊免費試用帳戶](#)。

先決條件

在本教學課程中，您將需要具有下列訂用帳戶的測試租使用者：

- Azure Active Directory Premium ([免費試用](#))
- 包含 Exchange ([免費試用](#)) 的 Microsoft 365 Apps 商務版訂用帳戶

開始之前，請遵循 [快速入門：建立 iOS/iPadOS 的電子郵件裝置設定檔](#) 中的步驟，建立 iOS 裝置的測試裝置設定檔。

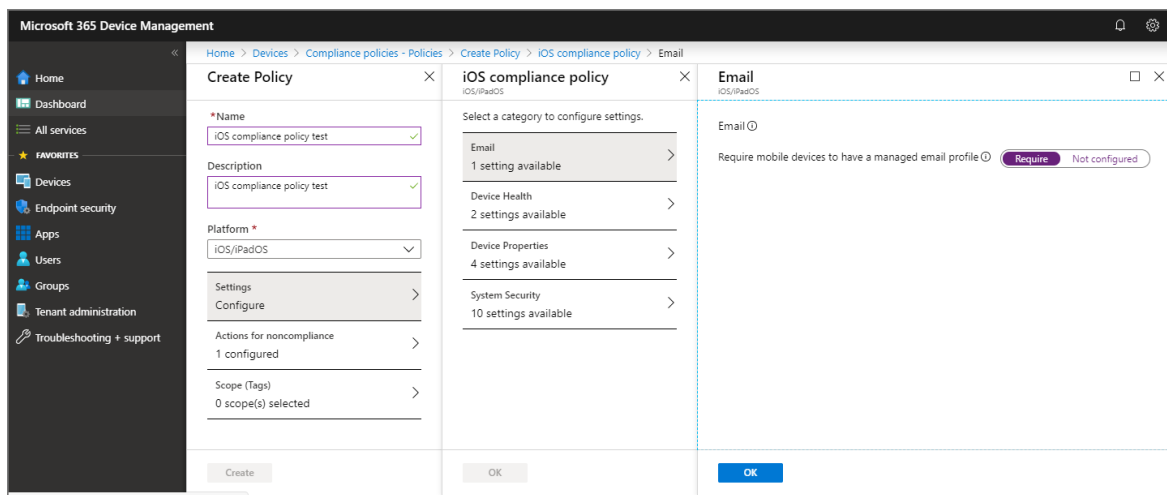
登入 Intune

以全域管理員或 Intune 服務系統管理員身分登入 [Microsoft 端點管理員 系統管理中心](#)。如果您已建立 Intune 試用版訂用帳戶，您使用 建立訂用帳戶 的帳戶就是全域管理員。

建立 iOS 裝置合規性政策

設定 Intune 裝置合規性原則，以設定裝置必須符合才能視為符合規範的條件。在本教學課程中，我們將建立 iOS 裝置的裝置合規性政策。合規性原則是平臺特定的，因此您需要針對您想要評估的每個裝置平臺使用個別的合規性政策。

1. 在 [Intune] 中，選取 [裝置 > 合規性原則 >] [建立原則]。
2. 針對 [名稱]，輸入 iOS 合規性政策測試。
3. 針對 [描述]，輸入 iOS 合規性政策測試。
4. 針對 [平臺]，選取 [iOS/iPadOS]。
5. 選取 > [設定 Email]。
 - a. 在 [需要行動裝置擁有受管理的電子郵件設定檔] 旁，選取 [需要]。
 - b. 選取 [確定]。



6. 選取 [裝置健康情況]。在 [已進行 JB 破解的裝置] 旁，選取 [封鎖]，然後選取 [確定]。

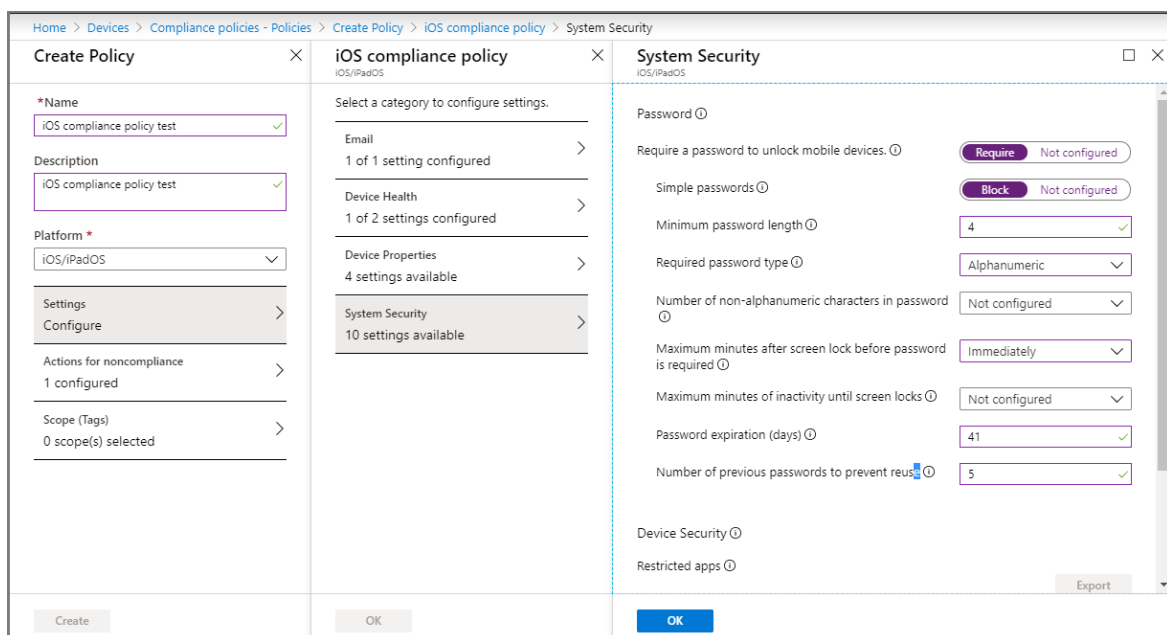
7. 選取 [系統安全性]，然後輸入 [密碼設定]。在本教學課程中，選取下列建議設定：

- 針對 [需要密碼以解除鎖定行動裝置]，選取 [需要]。
- 針對 [簡單密碼]，選取 [封鎖]。
- 針對 [密碼長度下限]，輸入 4。

TIP

呈現灰色並斜體化的預設值只是建議。您必須取代建議的值，才能設定設定。

- 針對 [必要密碼類型]，選擇 [英數位元]。
- 針對 [需要密碼之前螢幕鎖定後的分鐘數上限]，選擇 [立即]。
- 針對 [密碼到期 (天)]，請輸入 41。
- 針對 [防止重複使用的先前密碼數目]，輸入 5。



8. 選取 [確定]，然後再次選取 [確定]。

9. 選取 [建立]。

建立條件式存取原則

現在，我們將建立條件式存取原則，要求所有裝置平臺必須先註冊Intune並遵守我們的Intune合規性原則，才能存取Exchange Online。我們也會要求 Outlook 應用程式進行電子郵件存取。條件式存取原則可在 Azure AD 入口網站或 Microsoft 端點管理員 系統管理中心中設定。因為我們已經在系統管理中心，所以我們會在這裡建立原則。

1. 在 Microsoft 端點管理員系統管理中心，選取 [端點安全 > 性條件式存取 > 新原則]。
2. 針對 [名稱]，輸入 Microsoft 365 電子郵件的測試原則。
3. 在 [指派] 底下，選取 [使用者和群組]。在 [包含] 索引標籤上，選取 [所有使用者]，然後選取 [完成]。
4. 在 [指派] 底下，選取 [雲端應用程式或動作]。因為我們想要保護 Microsoft 365 Exchange Online電子郵件，所以我們會遵循下列步驟加以選取：
 - a. 在 [包含] 索引標籤上，選擇 [選取應用程式]。
 - b. 選擇 [選取]。
 - c. 在應用程式清單中，選取 [Office 365 Exchange Online]，然後選擇 [選取]。
 - d. 選取 [完成]。

The screenshot displays the 'New' policy configuration window in the Microsoft Endpoint Manager console. The window is divided into three main sections: 'Info', 'Cloud apps or actions', and 'Select'.

- Info:** Contains the 'Name' field with the value 'Test policy for Office 365 email'. Below it are sections for 'Assignments' (Users and groups, All users), 'Cloud apps or actions' (No cloud apps or actions selected), 'Conditions' (0 conditions selected), 'Access controls' (Grant, 0 controls selected; Session, 0 controls selected), and 'Enable policy' (On/Off toggle).
- Cloud apps or actions:** Contains a section 'Select what this policy applies to' with 'Cloud apps' selected. Below it are 'Include' and 'Exclude' tabs, and a list of options: 'None', 'All cloud apps', and 'Select apps' (selected). A 'Select None' button is also present.
- Select:** Contains a list of applications. 'Office 365 Exchange Online' is selected. Other applications listed include Microsoft Cloud App Security, Microsoft Intune, Microsoft Intune Enrollment, Microsoft Search in Bing, Microsoft.MileIQ.Dashboard, Office 365 SharePoint Online, Outlook Groups, and Skype for Business Online. A 'Selected' summary shows 'Office 365 Exchange Online'.

Buttons at the bottom include 'Create', 'Done', and 'Select'.

5. 在 [指派] 底下，選取 [條件 > 裝置平臺]。
 - a. 在 [設定] 底下，選取 [是]。
 - b. 在 [包含] 索引標籤上，選取 [任何裝置]，然後選取 [完成]。
 - c. 再次選取 [完成]。

Home > Endpoint security > Conditional Access - Policies > New > Conditions > Device platforms

New	Conditions	Device platforms
Info Name * Test policy for Office 365 email ✓ Assignments Users and groups ① All users > Cloud apps or actions ① 1 app included > Conditions ① 1 condition selected > Access controls Grant ① 0 controls selected > Session ① 0 controls selected > Enable policy On Off Create	Info Sign-in risk ① Not configured > Device platforms ① Any device > Locations ① Not configured > Client apps (Preview) ① Not configured > Device state (Preview) ① Not configured > Done	Apply policy to selected device platforms. Learn more Configure ① Yes No Include Exclude ☒ Any device ☐ Select device platforms ☐ Android ☐ iOS ☐ Windows Phone ☐ Windows ☐ macOS Done

6. 在 [指派] 底下，選取 [條件 > 用戶端應用程式]。

a. 在 [設定] 底下，選取 [是]。

b. 在本教學課程中，請選取 [行動應用程式和桌面客戶端] 和 [新式驗證客戶端 (參照 iOS 版 Outlook 和 Android 版 Outlook) 等應用程式。清除所有其他核取方塊。

c. 選取 [完成]，然後再次選取 [完成]。

Home > Endpoint security > Conditional Access - Policies > New > Conditions > Client apps (Preview)

New	Conditions	Client apps (Preview)
Info Name * Test policy for Office 365 email ✓ Assignments Users and groups ① All users > Cloud apps or actions ① 1 app included > Conditions ① 1 condition selected > Access controls Grant ① 0 controls selected > Session ① 0 controls selected > Create	Info Sign-in risk ① Not configured > Device platforms ① Any device > Locations ① Not configured > Client apps (Preview) ① Not configured > Device state (Preview) ① Not configured > Done	Configure ① Yes No Select the client apps this policy will apply to ☐ Browser ☒ Mobile apps and desktop clients ☒ Modern authentication clients ☐ Exchange ActiveSync clients ☐ Other clients ① Done

7. 在 [存取控制] 底下，選取 [授與]。

- 在 [授與] 窗格上，選取 [授與存取權]。
- 選取 [需要將裝置標示為符合規範]。
- 選取 [需要核准的用戶端應用程式]。
- 在 [針對多個控制項] 下，選取 [需要所有選取的控制項]。此設定可確保當裝置嘗試存取電子郵件時，會強制執行您選取的兩個需求。
- 選擇 [選取]。

Home > Endpoint security > Conditional Access - Policies > New > Grant

New [X] **Grant** [] [X]

Info

Name *
Test policy for Office 365 email ✓

Assignments

Users and groups ⓘ
All users >

Cloud apps or actions ⓘ
1 app included >

Conditions ⓘ
2 conditions selected >

Access controls

Grant ⓘ
0 controls selected >

Session ⓘ
0 controls selected >

Enable policy

On Off

Select the controls to be enforced.

☐ Block access

☒ Grant access

☐ Require multi-factor authentication ⓘ

☒ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☒ Require approved client app ⓘ
[See list of approved client apps](#)

☐ Require app protection policy (Preview) ⓘ
[See list of policy protected client apps](#)

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

⚠ Don't lock yourself out! Make sure that your device is compliant.

Create Select

- 在 [啟用原則] 下，選取 [開啟]。

Enable policy

On Off

- 選取 [建立]。

進行測試

使用您已建立的原則，任何嘗試登入 Microsoft 365 電子郵件的 iOS 裝置都必須註冊Intune，並使用適用於 iOS/iPadOS 的 Outlook 行動裝置應用程式。若要在 iOS 裝置上測試此案例，請嘗試使用測試租使用者中使用者的認證登入Exchange Online。系統會提示您註冊裝置並安裝 Outlook 行動裝置應用程式。

1. 若要在 iPhone 上測試，請移至 [設定 > 密碼&帳戶 > 新增帳戶 > 交換]。
2. 輸入測試租使用者中使用者的電子郵件地址，然後按 [下一步]。
3. 按 [登入]。
4. 輸入測試使用者的密碼，然後按 [登入]。
5. 出現一則訊息，指出您的裝置必須受管理才能存取資源，以及註冊選項。

清除資源

當不再需要測試原則時，您可以將它們移除。

1. 以全域管理員或Intune服務管理員身分登入[Microsoft 端點管理員 系統管理中心](#)。
2. 選取 [裝置 > 合規性原則]。
3. 在 [原則名稱] 清單中，選取測試原則的操作功能表 (...)，然後選取 [刪除]。選取 [確定] 以確認。
4. 選取 [端點安全 > 性條件式存取]。
5. 在 [原則名稱] 清單中，選取測試原則的操作功能表 (...)，然後選取 [刪除]。選取 [是] 加以確認。

後續步驟

在本教學課程中，您已建立原則，要求 iOS 裝置註冊Intune，並使用 Outlook 應用程式來存取Exchange Online電子郵件。若要瞭解如何搭配條件式存取使用Intune來保護其他應用程式和服務，包括Exchange ActiveSync Microsoft 365 Exchange Online的用戶端，請參閱[設定條件式存取](#)。

教學課程：保護非受控裝置上 Exchange Online 電子郵件

2022/9/27 •

在本教學課程中，您將瞭解如何使用應用程式保護原則搭配條件式存取來保護 Exchange Online，即使裝置未在裝置管理解決方案中註冊，例如 Intune。在本教學課程中，您將瞭解如何：

- 為 Outlook 應用程式建立 Intune 應用程式保護原則。您將防止「另存新檔」並限制剪下、複製和貼上動作，以限制使用者可以對應用程式資料執行的動作。
- 建立 Azure Active Directory (Azure AD) 條件式存取原則，只允許 Outlook 應用程式存取 Exchange Online 中的公司電子郵件。您也需要多重要素驗證 (新式驗證用戶端的 MFA)，例如 iOS 版 Outlook 和 Android 版。

先決條件

在本教學課程中，您將需要具有下列訂閱帳戶的測試租使用者：

- Azure Active Directory Premium (免費試用)
- Intune 免費試用 (訂閱帳戶)
- 包含 Exchange (免費試用) 的 Microsoft 365 Apps 商務版訂閱帳戶

登入 Intune

在本教學課程中，當您登入 [Microsoft 端點管理員 系統管理中心](#) 時，請以 [全域管理員](#) 或 [Intune 服務系統管理員身分登入](#)。如果您已建立 Intune 試用版訂閱帳戶，您使用 建立訂閱帳戶的帳戶就是全域管理員。

建立應用程式保護原則

在本教學課程中，我們將針對適用於 Outlook 應用程式的 iOS 設定 Intune [應用程式保護原則](#)，以在應用層級設定保護。我們需要 PIN 才能在工作內容中開啟應用程式。我們也會限制應用程式之間的資料共用，並防止公司資料儲存到個人位置。

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 > 應用程式防護 > 原則建立原則]，然後針對平臺選取 [iOS/iPadOS]。
3. 在 [基本] 頁面上，設定下列設定：

- 名稱：輸入 Outlook 應用程式原則測試。
- 描述：輸入 Outlook 應用程式原則測試。

[平臺] 值會設定為您先前的選擇。

按 [下一步] 繼續。

4. [應用程式]**** 頁面可讓您選擇如何將此原則套用至不同裝置上的應用程式。設定下列選項：

- 針對 [目標至所有應用程式類型]：選取 [否]，然後針對 [應用程式類型]，選取 [非受控裝置上的應用程式] 複選框。
- 按一下 [選取公用應用程式]。在 [應用程式] 清單中，選取 [Microsoft Outlook]，然後選擇 [選取]。Microsoft Outlook 現在會出現在 [公用應用程式] 底下。

按 [下一步] 繼續。

5. [資料保護] 頁面提供的設定可決定使用者如何與套用此應用程式保護原則之應用程式中的資料互動。設

定下列選項：

在 [資料傳輸] 下方，設定下列設定，將所有其他設定保留為其預設值：

- 針對 [將組織資料傳送至其他應用程式]，選取 [無]。
- 針對 [從其他應用程式接收資料]，選取 [無]。
- 針對 [限制其他應用程式之間的剪下、複製和貼上]，選取 [已封鎖]。

Microsoft Endpoint Manager admin center

Home > Apps > Create policy ...

Basics Apps **Data protection** Access requirements Conditional launch Scope tags Assignments Review + create

This group includes the data loss prevention (DLP) controls, like cut, copy, paste, and save-as restrictions. These settings determine how users interact with data in the apps.

Data Transfer

Backup org data to iTunes and iCloud backups ☒ Allow ☐ Block

Send org data to other apps ☒ None

Select apps to exempt

Save copies of org data ☒ Allow ☐ Block

Allow user to save copies to selected services ☒ 0 selected

Transfer telecommunication data to ☒ Any dialer app

Dialer App URL Scheme

Receive data from other apps ☒ None

Open data into Org documents ☒ Allow ☐ Block

Allow users to open data from selected services ☒ 3 selected

Restrict cut, copy, and paste between other apps ☒ Blocked

Cut and copy character limit for any app

Third party keyboards ☒ Allow ☐ Block

Encryption

Encrypt org data ☒ Require ☐ Not required

Functionality

Sync policy managed app data with native apps ☒ Allow ☐ Block

Printing org data ☒ Allow ☐ Block

Restrict web content transfer with other apps ☒ Any app

Unmanaged browser protocol ☒

Org data notifications ☒ Allow

選取 [下一步] 繼續。

6. [存取需求] 頁面提供設定，可讓您設定使用者在工作內容中存取應用程式時必須符合的 PIN 和認證需求。設定下列設定，將所有其他設定保留為其預設值：

- 針對 [PIN 以進行存取]，選取 [需要]。
- 針對 [公司或學校帳號憑證] 進行存取，選取 [需要]。

選取 [下一步] 繼續。

7. [條件式啟動] 頁面提供設定，以設定應用程式保護原則的登入安全性需求。在本教學課程中，您不需要設定這些設定。

按 [下一步] 繼續。

8. 使用 [指派] 頁面將應用程式保護原則指派給使用者群組。在本教學課程中，您不會將此原則指派給群組。

按 [下一步] 繼續。

9. 在 [下一步：檢閱 + 建立] 頁面上，檢閱您為此應用程式保護原則輸入的值和設定。按一下 [建立] 以在 Intune 中建立應用程式保護原則。

已建立 Outlook 的應用程式保護原則。接下來，您將設定條件式存取，以要求裝置使用 Outlook 應用程式。

建立條件式存取原則

現在，我們將使用 Microsoft 端點管理員 系統管理中心來建立兩個條件式存取原則，以涵蓋所有裝置平臺。您將[條件式存取與Intune整合](#)，以協助控制可連線到電子郵件和公司資源的裝置和應用程式。

- 第一個原則會要求新式驗證用戶端使用核准的 Outlook 應用程式和多重要素驗證 (MFA)。新式驗證用戶端包括 iOS 版 Outlook 和 Android 版 Outlook。
- 第二個原則會要求Exchange ActiveSync用戶端使用核准的 Outlook 應用程式。(目前，Exchange Active Sync 不支援裝置平臺) 以外的條件。您可以在 Azure AD 入口網站或 Microsoft 端點管理員 系統管理中心

設定條件式存取原則。因為我們已經在系統管理中心，所以我們會在這裡建立原則。

當您在 Microsoft 端點管理員 系統管理中心設定條件式存取原則時，您實際上是在 Azure 入口網站的 [條件式存取] 刀鋒視窗中設定這些原則。因此，使用者介面與您為 Intune 設定其他原則時稍有不同。

建立新式驗證用戶端的 MFA 原則

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [端點安全 > 性條件式存取 >][新增原則]。
3. 針對 [名稱]，輸入 新式驗證用戶端的測試原則。
4. 在 [指派] 底下，選取 [使用者和群組]。在 [包含] 索引標籤上，選取 [所有使用者]，然後選取 [完成]。
5. 在 [指派] 底下，選取 [雲端應用程式或動作]。因為我們想要保護 Microsoft 365 Exchange Online 電子郵件，所以我們會遵循下列步驟加以選取：
 - a. 在 [包含] 索引標籤上，選擇 [選取應用程式]。
 - b. 選擇 [選取]。
 - c. 在 [應用程式] 清單中，選取 [Office 365 Exchange Online]，然後選擇 [選取]。
 - d. 選取 [完成] 以返回 [新增原則] 窗格。

The screenshot displays the 'New' Conditional Access policy configuration page in the Microsoft Endpoint Manager console. The page is divided into several sections: 'Name' (with a text input field containing 'Test policy for modern auth clients'), 'Assignments' (with a dropdown for 'Users and groups' set to 'All users'), 'Cloud apps or actions' (with a dropdown for 'Cloud apps or actions' set to 'No cloud apps, actions, or authentication contexts selected'), 'Conditions' (with a dropdown for 'Conditions' set to '0 conditions selected'), and 'Access controls' (with a dropdown for 'Access controls' set to '0 controls selected'). The 'Cloud apps or actions' section is highlighted with a red box, showing a list of cloud apps with 'Office 365 Exchange Online' selected. A 'Select' dialog box is open on the right, showing the same list of cloud apps with 'Office 365 Exchange Online' selected. The 'Selected items' section at the bottom of the dialog shows 'Office 365 Exchange Online' with a 'Remove' button.

6. 在 [指派] 底下，選取 [條件 > 裝置平臺]。
 - a. 在 [設定] 底下，選取 [是]。
 - b. 在 [包含] 索引標籤上，選擇 [選取裝置平臺]，然後選取 [Android 和 iOS]。
 - c. 選取 [完成]。
7. 在 [條件] 窗格上，選取 [用戶端應用程式]。
 - a. 在 [設定] 底下，選取 [是]。

- b. 選取 [行動應用程式和桌面用戶端] 和 [新式驗證用戶端]。
- c. 清除其他核取方塊。
- d. 選取 [完成 >] 以返回 [新增原則] 窗格。

Home > Endpoint security > Conditional Access >

New

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Test policy for modern auth clients ✓

Assignments

Users and groups ⓘ

All users

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only On Off

Create

User risk ⓘ

Not configured

Sign-in risk ⓘ

Not configured

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Device state (Preview) ⓘ

Not configured

Client apps

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ

Yes No

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser

☒ Mobile apps and desktop clients

Legacy authentication clients

☐ Exchange ActiveSync clients ⓘ

☐ Other clients ⓘ

Done

8. 在 [存取控制] 底下, 選取 [授與]。
- a. 在 [授與] 窗格上, 選取 [授與存取權]。
 - b. 選取 [需要多重要素驗證]。
 - c. 選取 [需要核准的用戶端應用程式]。
 - d. 在 [針對多個控制項] 下, 選取 [需要所有選取的控制項]。此設定可確保當裝置嘗試存取電子郵件時, 會強制執行您選取的兩個需求。
 - e. 選擇 [選取]。

New

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Test policy for modern auth clients ✓

Assignments

Users and groups ⓘ

[All users](#)

Cloud apps or actions ⓘ

[1 app included](#)

Conditions ⓘ

[1 condition selected](#)

Access controls

Grant ⓘ

[2 controls selected](#)

Session ⓘ

[0 controls selected](#)

Enable policy

Report-only **On** Off

Create

Grant



Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☒ Require approved client app ⓘ

[See list of approved client apps](#)

☐ Require app protection policy ⓘ

[See list of policy protected client apps](#)

☐ Require password change ⓘ

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Select

9. 在 [啟用原則] 底下, 選取 [開啟], 然後選取 [建立]。

New ...

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Test policy for modern auth clients ✓

Assignments

Users and groups ⓘ

All users

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

2 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only

On

Off

Create

系統會建立新式驗證用戶端的條件式存取原則。現在您可以建立 Exchange Active Sync 用戶端的原則。

建立 Exchange Active Sync 用戶端的原則

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [端點安全 > 性條件式存取 > 新原則]。
3. 針對 [名稱]，輸入 EAS 用戶端的測試原則。
4. 在 [指派] 底下，選取 [使用者和群組]。在 [包含] 索引標籤上，選取 [所有使用者]，然後選取 [完成]。
5. 在 [指派] 底下，選取 [雲端應用程式或動作]。選取具有下列步驟的 Microsoft 365 Exchange Online 電子郵件：
 - a. 在 [包含] 索引標籤上，選擇 [選取應用程式]。
 - b. 選擇 [選取]。
 - c. 從 [應用程式] 清單中，選取 [Office 365 Exchange Online]，然後選擇 [選取]，然後選擇 [完成]。
6. 在 [指派] 底下，選取 [條件 > 裝置平臺]。
 - a. 在 [設定] 底下，選取 [是]。
 - b. 在 [包含] 索引標籤上，選取 [任何裝置]，然後選取 [完成]。
7. 在 [條件] 窗格上，選取 [用戶端應用程式]。
 - a. 在 [設定] 底下，選取 [是]。

- b. 選取 [行動應用程式和桌面用戶端]。
- c. 選 Exchange ActiveSync用戶端。
- d. 清除所有其他核取方塊。
- e. 選取 [完成]，然後再次選取 [完成]。

New ...
Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
Test policy for EAS clients ✓

Assignments

Users and groups ⓘ
All users

Cloud apps or actions ⓘ
1 app included

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ
0 controls selected

Control user access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ
Not configured

Sign-in risk ⓘ
Not configured

Device platforms ⓘ
Not configured

Locations ⓘ
Not configured

Client apps ⓘ
Not configured

Device state (Preview) ⓘ
Not configured

Client apps ✕

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure ⓘ
Yes No

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser

☒ Mobile apps and desktop clients

Legacy authentication clients

☒ Exchange ActiveSync clients ⓘ

☐ Other clients ⓘ

8. 在 [存取控制] 底下，選取 [授與]。
 - a. 在 [授與] 窗格上，選取 [授與存取權]。
 - b. 選取 [需要核准的用戶端應用程式]。清除所有其他核取方塊。
 - c. 選擇 [選取]。

New

Conditional Access policy

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

Test policy for EAS clients

Assignments

Users and groups ⓘ

All users

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Grant



Control user access enforcement to block or grant access. [Learn more](#)

- ☐ Block access
- ☒ Grant access

☐ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☒ Require approved client app ⓘ
[See list of approved client apps](#)

☐ Require app protection policy ⓘ
[See list of policy protected client apps](#)

☐ Require password change ⓘ

For multiple controls

- ☒ Require all the selected controls
- ☐ Require one of the selected controls

9. 在 [啟用原則] 底下，選取 [開啟]，然後選取 [建立]。

您的應用程式保護原則和條件式存取現在已就緒且可供測試。

進行測試

使用您已建立的原則，裝置必須註冊Intune，並使用 Outlook 行動應用程式來存取 Microsoft 365 電子郵件。若要在 iOS 裝置上測試此案例，請嘗試使用測試租使用者中使用者的認證登入Exchange Online。

1. 若要在 iPhone 上測試，請移至 [設定 > 密碼&帳戶 > 新增帳戶 > 交換]。
2. 輸入測試租使用者中使用者的電子郵件地址，然後按 [下一步]。
3. 按 [登入]。
4. 輸入測試使用者的密碼，然後按 [登入]。
5. [需要更多資訊] 訊息隨即出現，這表示系統會提示您設定 MFA。繼續並設定其他驗證方法。
6. 接下來，您會看到一則訊息，指出您正嘗試使用 IT 部門未核准的應用程式來開啟此資源。訊息表示您遭到封鎖，無法使用原生郵件應用程式。取消登入。
7. 開啟 Outlook 應用程式，然後選取 > [設定][新增帳戶 >][新增Email帳戶]。
8. 輸入測試租使用者中使用者的電子郵件地址，然後按 [下一步]。
9. 按 [使用 Office 365 登入]。系統會提示您進行其他驗證和註冊。登入之後，您可以測試剪下、複製、貼上和「另存新檔」等動作。

清除資源

當不再需要測試原則時，您可以將它們移除。

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [裝置****合規性原則]。
3. 在 [原則名稱] 清單中，選取測試原則的操作功能表 (...)，然後選取 [刪除]。選取 [確定] 以確認。
4. 選取 [端點安全 > 性條件式存取]。
5. 在 [原則名稱] 清單中，選取每個測試原則 (...) 操作功能表，然後選取 [刪除]。選取 [是] 加以確認。

後續步驟

在本教學課程中，您已建立應用程式保護原則來限制使用者可以使用 Outlook 應用程式執行的動作，並建立了條件式存取原則來要求 Outlook 應用程式，並要求新式驗證用戶端使用 MFA。若要深入瞭解如何使用Intune與條件式存取來保護其他應用程式和服務，請參閱[瞭解條件式存取和Intune](#)。

教學課程：設定使用 Intune 進行 EMM 和應用程式設定的寬延時間

2022/9/27 •

時差是可與 Microsoft Intune 搭配使用的共同作業應用程式。

在本教學課程中，您將：

- 在您的寬延時間 Enterprise 格線上，將 Intune 設定為 Enterprise 行動性管理 (EMM) 提供者。您可以將格線計畫的工作區存取許可權制于 Intune 受管理的裝置。
- 建立應用程式設定原則，以管理適用於 iPadOS/的 EMM iOS 應用程式的寬限時間，以及 Android 個人擁有的工作設定檔裝置的寬延能力應用程式。
- 建立 Intune 裝置相容性原則，設定 Android 和 iOS/iPadOS 裝置必須符合的條件，以視為相容性。

如果您沒有 Intune 訂閱，請 [註冊免費試用帳戶](#)。

必要條件

使用此教學課程的下列訂閱時，您將需要測試租使用者：

- Azure Active Directory Premium ([免費試用版](#))
- Intune 訂閱 ([免費試用版](#))

您也需要[Enterprise 格線計畫的寬限時間](#)。

設定寬限 Enterprise 格線計畫

依[延後的指示](#)開啟 EMM，Enterprise 格線計畫，並以格線計畫的身分識別提供者的身分[Azure Active Directory \(IDP\)](#)。

登入 Intune

以全域管理員或 Intune 服務管理員身分登入[Microsoft 端點管理員系統管理中心](#)。如果您已建立 Intune 試用訂閱，您用來建立訂閱的帳戶即為全域管理員。

為 iOS 裝置上的 EMM 設定寬限時間

將 EMM 的 iOS/iPadOS 應用程式寬限新增至 Intune 租使用者，並建立應用程式設定原則，以讓您的組織的 iOS/iPadOS 使用者能夠使用 Intune 作為 EMM 提供者來存取寬限。

將 EMM 應用程式的 iOS/iPadOS 寬限時間新增至 Intune

在 Intune 中將 EMM 新增為受管理的 iOS/iPadOS 應用程式，並為您指派寬限使用者。應用程式是平臺特有的，所以您需要為您的 Android 裝置上的可寬限使用者新增個別的 Intune 應用程式。

1. 在 [Microsoft 端點管理員系統管理中心](#)，選取 [應用程式] [> > 新增]。
2. 在 [應用程式類型] 下，選擇 [iOS 儲存應用程式]，然後按一下 [選取]。
3. 按一下 [搜尋應用程式存放區]。輸入搜尋字詞 "EMM 的寬限時間"，然後選取應用程式。在 [搜尋應用程式存放區] 窗格中，按一下 [選取]。
4. 在 [應用程式資訊] 步驟中，視您所見，設定任何變更。選取 [下一步] 以設定您的應用程式資訊。
5. 在 [工作分派] 步驟中，按一下 [必要] 區段下的 [新增群組]。選取一個或多個要指派應用程式的群組。完成

時，按 [下一步] 繼續。

6. 在 [複查 + 建立] 步驟中，在驗證應用程式詳細資料之後，按一下 [建立]。

為 EMM 應用程式的自動寬限新增 iOS/iPadOS 應用程式佈建原則

為 EMM 應用程式的 iOS/iPadOS 寬限新增應用程式設定原則。> [!NOTE] > App configuration policies for managed devices are platform-specific, so you need to add a separate policy for your Slack users on Android devices.

1. 在 [Microsoft 端點管理員系統管理中心](#)，選取 [應用 > 程式應用程式設定原則] [> 新增 > 受管理的裝置]。
2. 在 [名稱] 中，輸入「時差應用程式設定原則測試」。
3. 在 [裝置註冊類型] 中，確認已設定 受管理的裝置。
4. 針對 [平臺]，選取 [iOS/iPadOS]。
5. 在 [目標應用程式] 中，按一下 [選取應用程式]。隨即會顯示 相關的應用程式 窗格。
6. 在搜尋列中，輸入「EMM 的寬延時間」，然後選取應用程式。按一下 [> 下一步]。
7. 在 設定 步驟中，設定設定 設定格式 以使用 configuration designer。
8. 新增 為設定機 碼。將 數值型別 設定為 字串，並將設定 值 設定為 。

NOTE

設定機 碼提供輸入組織的 URL 網域，以協助使用者登入的功能。

9. 按一下 [下一步]。
10. 在 [工作分派] 步驟中，按一下 [所有使用者]。然後按一下「下一步」。
11. 在 [複查 + 建立] 步驟中，按一下 [建立] 以建立設定原則。

(選用) 建立 iOS 裝置合規性原則

設定 Intune 裝置相容性原則，設定裝置必須符合的條件，以視為相容性。針對此教學課程，我們會為 iOS/iPadOS 裝置建立裝置合規性原則。規範原則是平臺特有的原則，因此您需要為您在 Android 裝置上為寬限使用者建立個別的原則。

1. 在 [Microsoft 端點管理員系統管理中心](#) 中，選取 [裝置 > 規範原則 > 原則] [> 建立原則]。
2. 選取 [iOS/iPadOS 做為 平臺]。然後按一下 [建立]。
3. 在 [基礎] 步驟中，輸入 "iOS 規範原則 test" 作為 名稱，然後按 [下一步]。
4. 在 [規範設定] 的 [裝置健康情況] 底下，選取 [已越獄裝置] 旁的 [封鎖]。
5. 在 [此教學的 系統安全性] 下，選取下列設定：
 - 若需要密碼才能解除鎖定行動裝置，請選取 [需要]。
 - 若為 簡單密碼，請選取 [封鎖]。
 - 若為 [最小密碼長度]，請輸入 。
 - 針對 [必要密碼類型]，選擇 [數位]。
 - 若要在需要密碼前的最大分鐘數之後，請選擇 [立即]。
 - 在 [密碼到期 (天數)] 中，輸入 。
 - 如需 舊密碼的數目以避免重複使用，請輸入 。
6. 按 [下一步]，然後再選取 [下一步]。
7. 在 [工作分派] 步驟中，按一下 [新增所有使用者]。然後按一下「下一步」。
8. 在 [複查 + 建立] 步驟中，按一下 [建立] 以建立相容性原則。

在 Android 個人擁有的工作設定檔裝置上設定寬限時間

將寬延時間管理的 Google Play 應用程式新增至您的 Intune 租使用者，並建立應用程式設定原則，以讓您的組織的 Android 使用者使用 Intune 作為 EMM 提供者來存取寬限。

將 Android 時差應用程式新增至 Intune

在 Intune 中將寬限新增為受管理的 Google Play 應用程式，並指定您的寬限使用者。應用程式是平臺特有的，所以您需要為 iOS/iPadOS 裝置上的可寬限使用者新增個別的 Intune 應用程式。

1. 在 [Microsoft 端點管理員系統管理中心](#)，選取 [應用程式] [> > 新增]。
2. 在 [應用程式類型] 下，選擇 [Managed Google Play App]，然後按一下 [選取]。
3. 在 搜尋 方塊中，輸入搜尋字詞 "時差"，然後選取應用程式。在 [管理 Google 播放] 窗格中，按一下 [核准]。按一下 [核准]，也核准應用程式的許可權。驗證應用程式的核准設定後，按一下 [完成]。按一下 [選取]。
4. 在 [所有應用程式] 窗格中，按一下 [重新整理] 以更新應用程式清單。然後，按一下 [新增 寬延時間] 應用程式。
5. 按一下 [工作分派] 旁的 [編輯]。
6. 如您所見，請設定任何變更。選取 [下一步] 以設定您的應用程式資訊。
7. 按一下 [必要] 區段下的 [新增群組]。選取一個或多個要指派應用程式的群組。完成時，按一下 [回顧 + 儲存]。
8. 在 [複查] [儲存] 步驟中，在驗證應用程式詳細資料之後，按一下 [儲存]。

新增時差的 Android 應用程式佈建原則

新增時差的應用程式設定原則。受管理裝置的應用程式設定原則是平臺特有的，所以您需要為 iOS/iPadOS 裝置上的寬限使用者新增個別的原則。

1. 在 [Microsoft 端點管理員系統管理中心](#)，選取 [應用 > 程式應用程式設定原則] [> 新增 > 受管理的裝置]。
2. 在 [名稱] 中，輸入「時差應用程式設定原則測試」。
3. 在 [裝置註冊類型] 中，確認已設定 受管理的裝置。
4. 在 [平臺] 中，選取 [Android Enterprise]。
5. 針對 [配置檔案類型]，選取 [僅限個人擁有的工作設定檔]。
6. 在 [目標應用程式] 中，按一下 [選取應用程式]。隨即會顯示 相關的應用程式 窗格。
7. 在搜尋列中，輸入 "時差"，然後選取 [Managed Google Play store] 應用程式。按一下 [> 下一步]。
8. 在 設定 步驟中，設定設定 設定格式 以使用 configuration designer。
9. 新增 為設定機 碼。按一下 [確定]。

NOTE

設定機 碼提供輸入組織的 URL 網域，以協助使用者登入的功能。

10. 按一下 [下一步]。
11. 在 [工作分派] 步驟中，按一下 [新增所有使用者]。然後按一下「下一步」。
12. 在 [複查 + 建立] 步驟中，按一下 [建立] 以建立設定原則。

(選用) 建立 Android 裝置合規性原則

設定 Intune 裝置相容性原則，設定裝置必須符合的條件，以視為相容性。針對此教學課程，我們將為 Android 裝置建立裝置規範原則。規範原則是平臺特有的，所以您需要為 iOS/iPadOS 裝置上的寬限使用者建立個別的原則。

1. 在 [Microsoft 端點管理員系統管理中心](#) 中，選取 [裝置 > 規範原則 > 原則] [> 建立原則]。
2. 選取 [Android Enterprise 當做 平臺]，然後選取 [個人擁有的工作設定檔] 做為 配置檔案類型。然後按一下 [建立]。
3. 在 [基礎] 步驟中，輸入 "Android Enterprise 規範原則 test" 作為 名稱，然後按 [下一步]。
4. 在 [規範設定] 的 [裝置健康情況] 底下，選取 [根裝置] 旁邊的 [封鎖]。
5. 在 [此教學的 系統安全性] 下，選取下列設定：
 - 若需要密碼才能解除鎖定行動裝置，請選取 [需要]。
 - 針對 [必要密碼類型]，請選擇 至少一個數位。

- 若為 [最小密碼長度]，請輸入 。
 - 在 [密碼到期前的天數] 中，輸入 。
 - 如需 舊密碼的數目以避免重複使用，請輸入 。
 - 若要在需要密碼前的最長空閒分鐘，請選擇 [15 分鐘]。
6. 按 [下一步]，然後再選取 [下一步] 。
 7. 在 [工作分派] 步驟中，按一下 [新增所有使用者]。然後按一下「下一步」。
 8. 在 [複查 + 建立] 步驟中，按一下 [建立] 以建立相容性原則。

啟動寬限時間

在您剛才建立的原則中，任何 iOS/iPadOS 或 Android 個人擁有的工作設定檔裝置，都必須進行 Intune 登錄才能登入其中一個工作區。若要測試此案例，請嘗試在 Intune 註冊的 iOS/iPadOS 裝置上啟動 EMM 的寬限時間，或在 Intune 已註冊的 Android 個人的工作設定檔裝置上啟動寬限時間。

後續步驟

在本教學課程中：

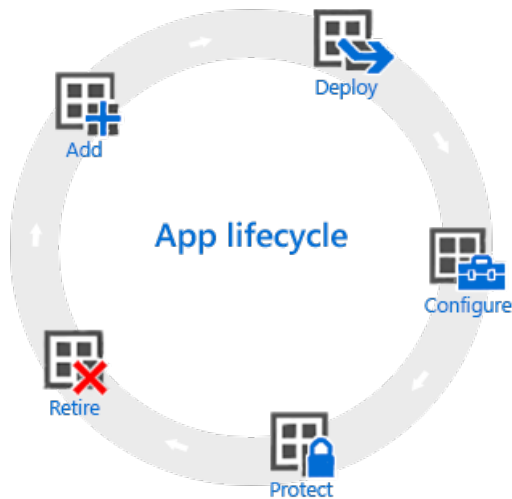
- 您可以在寬限時間 Enterprise 格線上，設定 Intune 做為 Enterprise 行動性管理 (EMM) 提供者。
- 您已建立應用程式設定原則，管理 iPadOS/的 EMM iOS 應用程式的寬限時間，以及 Android 個人擁有的工作設定檔裝置的寬延能力應用程式。
- 您已建立 Intune 裝置相容性原則，設定 Android 和 iOS/iPadOS 裝置必須符合的條件，以視為相容性。

若要深入瞭解應用程式設定原則，請參閱[Microsoft Intune 的應用程式佈建原則](#)。若要深入瞭解裝置規範原則，請參閱 [在裝置上設定規則，以允許使用 Intune 存取您組織中的資源](#)。

Microsoft Intune 中的應用程式生命週期一覽

2022/9/27 •

Microsoft Intune 應用程式生命週期會在應用程式新增時開始，並在其他階段執行，直到您移除應用程式為止。瞭解這些階段後，您將具備 Intune 中開始使用應用程式管理所需的詳細資料。



新增

應用程式部署的第一個步驟是將您想要管理及指派的應用程式新增至 Intune。雖然您可以使用許多不同的應用程式類型，但基本程式是相同的。使用 Intune 您可以新增不同的應用程式類型，包括在內部 (企業營運) 的應用程式、儲存區中的應用程式、內建的應用程式，以及網路上的應用程式。如需每個應用程式類型的詳細資訊，請參閱 [how to add a app to Microsoft Intune](#)。

部署

在您將應用程式新增至 Intune 後，您可以將其指派給您管理的使用者和裝置。Intune 使此程式變得簡單，而且在部署應用程式之後，您可以從入口網站的 Intune [監視部署是否成功](#)。此外，在某些應用程式存放區中 (例如 [Apple](#) 和 [Windows](#) 應用程式存放區)，您可以為貴公司大量購買應用程式授權。Intune 可以與這些市集同步處理資料，以便讓您直接從 Intune 管理主控台部署及追蹤這些應用程式類型的授權使用方式。

設定

應用程式生命週期中會定期發行新的應用程式版本。Intune 提供的工具可輕鬆更新已部署至較新版本的 [應用程式](#)。此外，您可以設定某些應用程式的額外功能，例如：

- 針對應用程式執行時所使用的相容 iOS/iPadOS 應用程式，提供 [iOS/iPadOS 應用程式設定原則](#)。例如，應用程式可能需要特定品牌設定，或是必須連線的伺服器名稱。
- [Managed browser 原則](#) 可協助您設定 [Microsoft Edge](#) 的設定，這會取代預設裝置瀏覽器，並可讓您限制使用者可以造訪的網站。

保護

Intune 提供多種方法協助保護您應用程式中的資料。主要方法如下：

- [條件式存取](#)，可根據您指定的條件來控制電子郵件和其他服務的存取權。條件包括裝置類型或符合您部署的 [裝置合規性原則](#)。

- [應用程式防護原則](#)可以搭配個別應用程式使用，以協助保護公司資料的使用。例如，您可以限制在未受管理的應用程式和您管理的應用程式之間複製資料，也可以讓應用程式在已越獄或根的裝置上執行。

淘汰

最後，您已部署的應用程式很可能會過期，必須加以移除。Intune 可讓您輕鬆地卸載應用程式。如需詳細資訊，請參閱 [卸載應用程式](#)。

後續步驟

- 深入瞭解[Microsoft Intune 中的應用程式管理](#)

Intune中 Android Enterprise 裝置上的行動應用程式管理和個人擁有的工作設定檔

2022/9/27 •

在許多組織中，系統管理員都面臨保護不同裝置上資源和資料的挑戰。其中一項挑戰是使用個人 Android Enterprise 裝置保護使用者的資源，也稱為攜帶您自己的裝置 (BYOD)。Microsoft Intune支援兩種 Android 部署案例，適用於攜帶您自己的裝置 (BYOD)：

- [Mobile Application Management \(MAM\)](#)
- [Android Enterprise個人擁有的工作設定檔](#)

MAM 和 Android Enterprise個人擁有的工作設定檔部署案例包含下列 BYOD 環境的重要功能：

- **保護和隔離組織管理的資料：**這兩個解決方案都會藉由對組織管理的資料強制執行資料外泄防護 (DLP) 控制來保護組織資料。這些保護可防止意外洩漏受保護的資料，例如終端使用者不小心將其共用至個人應用程式或帳戶。它們也可確保存取資料的裝置狀況良好且不會遭到入侵。
- **使用者隱私 權：**MAM 會分隔受控應用程式中的使用者和組織內容，而 Android Enterprise個人擁有的工作設定檔會分隔裝置上的使用者內容，以及由行動裝置管理所管理 (MDM) 系統管理員所管理的資料。在這兩種情況下，IT 系統管理員都會強制執行原則，例如組織管理的應用程式或身分識別上的僅限 PIN 驗證。IT 系統管理員無法讀取、存取或清除終端使用者擁有或控制的資料。

無論您為 BYOD 部署選擇 MAM 或 Android Enterprise個人擁有的工作設定檔，都取決於您的需求和商務需求。本文的目標是提供指引來協助您決定。如需受控 Android 裝置的詳細資訊，請[參閱使用 Intune 管理 Android 個人擁有/公司擁有的工作設定檔裝置](#)。

關於Intune應用程式保護原則

Intune應用程式保護原則 (應用程式) 是以使用者為目標的資料保護原則。這些原則會在應用層級套用資料遺失保護。Intune應用程式需要應用程式開發人員在他們建立的應用程式上啟用應用程式功能。

個別的 Android 應用程式會透過幾種方式為 APP 啟用：

1. **原生整合到 Microsoft 第一方應用程式：**Microsoft Office適用於 Android 的應用程式，以及其他 Microsoft 應用程式的選取專案，隨附Intune應用程式內建。這些Office應用程式，例如 Word、OneDrive、Outlook 等，不需要再進行任何自訂即可套用原則。使用者可以直接從 Google Play 商店安裝這些應用程式。
2. **由開發人員使用 Intune SDK 整合到應用程式組建 中：**應用程式開發人員可以將Intune SDK 整合到其原始程式碼，並重新編譯其應用程式，以支援Intune應用程式原則功能。
3. **使用Intune應用程式包裝工具組裝：**有些客戶會編譯 Android 應用程式 (.APK 檔案) 不存取原始程式碼。如果沒有原始程式碼，開發人員就無法與 Intune SDK 整合。如果沒有 SDK，他們就無法針對 APP 原則啟用其應用程式。開發人員必須修改或重新編碼應用程式，才能支援 APP 原則。

為了提供協助，Intune包含現有 Android 應用程式 (AKS) 的 App Wrapping Tool工具，並建立可辨識 APP 原則的應用程式。

如需此工具的詳細資訊，請參閱 [準備應用程式保護原則的企業營運應用程式](#)。

若要查看已啟用 APP 的應用程式清單，請參閱 [具有一組豐富行動應用程式保護原則的受控應用程式](#)。

部署案例

本節說明 MAM 和 Android Enterprise個人擁有工作設定檔部署案例的重要特性。

MAM

MAM 部署會在應用程式上定義原則，而不是在裝置上定義原則。針對 BYOD，MAM 通常用於未註冊的裝置上。為了保護應用程式和存取組織資料，系統管理員會使用 APP 可管理的應用程式，並將資料保護原則套用至這些應用程式。

本功能適用於：

- Android 4.4 和更新版本

TIP

如需詳細資訊，請 [參閱什麼是應用程式保護原則？](#)。

Android Enterprise個人擁有的工作設定檔

Android Enterprise個人擁有的工作設定檔是核心 Android Enterprise部署案例。Android Enterprise個人擁有的工作設定檔是在 Android OS 層級建立的個別分割區，可由Intune管理。

Android Enterprise個人擁有的工作設定檔包含下列功能：

- **傳統 MDM 功能**：在任何 Android Enterprise案例中都提供重要的 MDM 功能，例如使用受控 Google Play 的應用程式生命週期管理。受控 Google Play 提供強大的體驗來安裝和更新應用程式，而不需要任何使用者介入。IT 也可以將應用程式組態設定推送至組織應用程式。它也不需要終端使用者允許來自未知來源的安裝。Android Enterprise個人擁有的工作設定檔提供其他常見的 MDM 活動，例如部署憑證、設定 WiFi/VPN，以及設定裝置密碼。
- **Android 上的 DLP Enterprise個人擁有的工作設定檔界限**：使用 Android Enterprise個人擁有的工作設定檔，DLP 原則會在工作設定檔層級強制執行，而不是在應用程式層級強制執行。例如，複製/貼上保護是由套用至應用程式的應用程式設定強制執行，或由工作設定檔強制執行。當應用程式部署至工作設定檔時，系統管理員可以在應用程式層級關閉此原則，以暫停工作設定檔的複製/貼上保護。

提示優化工作設定檔體驗

使用 Android Enterprise個人擁有的工作設定檔時，您應該考慮如何使用 APP 和多重身分識別。

在 Android 內使用 APP 的時機Enterprise個人擁有的工作設定檔

Intune APP 和 Android Enterprise個人擁有的工作設定檔是可一起或個別使用的互補技術。在架構上，這兩個解決方案都會在不同的層級強制執行原則 – 個別應用層的 APP，以及設定檔層的工作設定檔。將使用 APP 原則管理的應用程式部署到工作設定檔中的應用程式是有效且支援的案例。使用 APP、工作設定檔或組合取決於您的 DLP 需求。

如果某個設定檔不符合貴組織的資料保護需求，Android Enterprise個人擁有的工作設定檔和 APP 會提供額外的涵蓋範圍，以補充彼此的設定。例如，工作設定檔不會以原生方式提供控制，以限制應用程式儲存至不受信任的雲端儲存位置。APP 包含這項功能。您可以決定僅由工作設定檔提供的 DLP 已足夠，並選擇不使用 APP。或者，您可能需要兩者組合的保護。

隱藏 Android Enterprise個人擁有工作設定檔的 APP 原則

您可能需要支援具有多個裝置的個別使用者 - 使用 MAM 受控應用程式取消註冊的裝置，以及使用 Android Enterprise個人擁有工作設定檔的受控裝置。

例如，您需要使用者在開啟工作應用程式時輸入 PIN。根據裝置，PIN 功能會由 APP 或工作設定檔處理。針對 MAM 受控應用程式，應用程式會強制執行包含 PIN 到啟動行為的存取控制。對於已註冊的裝置，可能會停用應用程式 PIN，以避免同時需要裝置 PIN 和應用程式 PIN。(Android的應用程式 PIN 設定。針對工作設定檔裝置，

您可以使用 OS 強制執行的裝置或工作設定檔 PIN。若要完成此案例，請設定應用程式設定，使其不會在應用程式部署到工作設定檔時套用。如果您未以這種方式進行設定，裝置會提示使用者輸入 PIN 碼，並在應用層再次提示使用者輸入 PIN 碼。

在 Android 中控制多重身分識別行為Enterprise個人擁有的工作設定檔

Office Outlook和OneDrive等應用程式具有「多重身分識別」行為。在應用程式的一個實例中，使用者可以將連線新增至多個不同的帳戶或雲端儲存體位置。在應用程式內，從這些位置擷取的資料可以分開或合併。此外，使用者可以在個人身分識別 (user@outlook.com) 與組織身分識別 (user@contoso.com) 之間進行內容切換。

使用 Android Enterprise個人擁有的工作設定檔時，您可能會想要停用此多重身分識別行為。當您停用它時，只能使用組織身分識別來設定工作設定檔中應用程式的徽章實例。使用 [允許的帳戶] 應用程式組態設定來支援 Office Android 應用程式。

如需詳細資訊，請[參閱部署 iOS/iPadOS 和 Android 應用程式組態設定的Outlook](#)。

使用 Intune APP 的時機

有數個企業行動性案例，其中使用 Intune APP 是最佳建議。

沒有 MDM、沒有註冊、Google 服務無法使用

有些客戶不想要任何形式的裝置管理，包括 Android Enterprise個人擁有的工作設定檔管理，原因不同：

- 法律和責任原因
- 使用者體驗的一致性
- Android 裝置環境具有高度異質性
- 對 Google 服務沒有任何連線能力，這是工作設定檔管理的必要專案。

例如，中國或有使用者的客戶無法使用 Android 裝置管理，因為 Google 服務遭到封鎖。在此情況下，請使用 Intune APP for DLP。

摘要

使用 Intune, MAM 和 Android Enterprise個人擁有的工作設定檔都適用於您的 Android BYOD 計畫。您可以選擇使用 MAM 和/或工作設定檔，視您的業務和使用需求而定。總而言之，如果您需要受管理裝置上的 MDM 活動，例如憑證部署、應用程式推送等，請使用 Android Enterprise個人擁有的工作設定檔。如果您想要保護應用程式內的組織資料，請使用 MAM。

後續步驟

[開始使用應用程式保護原則](#)，或 [註冊您的裝置](#)。

如何在沒有 Google 行動服務的環境中使用Intune

2022/9/27 •

Microsoft Intune使用 Google Mobile Services (GMS)，在管理 Android 裝置時與Microsoft Intune公司入口網站通訊。在某些情況下，裝置可能暫時或永久無法存取 GMS。例如，裝置可能在沒有 GMS 的情況下寄送，或裝置可能連線到無法使用 GMS 的已關閉網路。本檔摘要說明您在安裝及使用 Intune來管理不含 GMS 的 Android 裝置時，可能會觀察到的差異和限制。

NOTE

這些 GMS 相關限制也適用於裝置系統管理員管理和 Android (AOSP) 管理。

在沒有 Google Play 商店存取權的情況下安裝Intune 公司入口網站應用程式

適用於人員中國以外的使用者

如果 Google Play 無法使用，Android 裝置可以下載[適用於 Android 的Microsoft Intune 公司入口網站](#)，並側載應用程式。以這種方式安裝時，應用程式不會自動收到更新或修正。您必須務必定期更新並手動修補應用程式。

適用於人員中的使用者

因為 Google Play 商店目前無法在人員的中國中使用，所以 Android 裝置必須從中文應用程式市集取得應用程式。如需詳細資訊，請參閱[在人員的中國安裝公司入口網站應用程式](#)。

當 GMS 無法使用時，Intune管理的限制

無法使用Intune功能

某些Intune功能依賴 GMS 的元件，例如 Google Play 商店或 Google Play 服務。因為在沒有 GMS 的環境中無法使用這些元件，Intune系統管理員主控台下的下列功能可能無法使用。

“	“
裝置合規性原則	建立或編輯 Android 裝置系統管理員的合規性原則時，Google Play Protect 下列出的所有選項都無法使用。
應用程式防護條件式啟動(原則)	SafetyNet  、  ，以及 ( ) 是無法用於條件式啟動的裝置條件。
用戶端應用程式	 Android 類型的應用程式。請改用  來部署和管理應用程式。
行動威脅防禦應用程式	請與您的 MTD 廠商合作，以瞭解其解決方案是否已與Intune整合、是否可在感興趣的區域中使用，以及其是否依賴 GMS。

某些工作可能會延遲

在可使用 GMS 的環境中，Intune依賴推播通知來加速工作完成。例如，如果您嘗試從遠端抹除裝置，通知通常會在幾秒內到達裝置。在無法使用 GMS 的情況下，推播通知可能也無法使用。因此，Intune必須等待下一個裝置簽入時間才能完成工作。

已註冊的 Android 裝置會每隔 8 小時報告Intune一次。例如，如果裝置在下午 1 點回報Intune，而遠端工作是在

下午 1:05 發出, Intune會在晚上 9 點連絡裝置以完成工作。

下列工作最多可能需要 8 小時才能完成：

Intune主控台：

- 完整抹除
- 選擇性抹除
- 新的或更新的應用程式部署
- 遠端鎖定
- 密碼重設

Intune 公司入口網站 Android 應用程式：

- 遠端裝置移除
- 裝置重設
- 安裝可用的企業營運應用程式

Intune適用於 Android (AOSP) 的應用程式：

- 遠端裝置移除
- 裝置重設

Intune 公司入口網站網站：

- 本機和遠端) (裝置移除
- 裝置重設
- 裝置密碼重設

如果裝置最近註冊, 合規性、不符合規範和設定簽入會更頻繁地執行。如需裝置簽入的詳細資訊, 請參閱[Microsoft Intune中裝置原則和設定檔的常見問題、問題和解決方式](#)。

後續步驟

- [使用 Microsoft Intune 將應用程式指派給群組](#)

將應用程式新增至 Microsoft Intune

2022/9/27 •

您必須先將應用程式新增至Microsoft Intune，才能設定、指派、保護或監視應用程式。

貴公司應用程式和裝置的使用者 (公司的員工) 可能有數個應用程式需求。將應用程式新增至Intune，並讓您的員工能夠使用之前，您可能會發現評估和瞭解一些應用程式基本概念很有說明。有各種類型的應用程式可供Intune 使用。您必須判斷公司使用者所需的應用程式需求，例如您的員工所需的平臺和功能。您必須判斷是否要使用Intune來管理裝置，(包括應用程式) 或Intune管理應用程式，而不需要管理裝置。此外，您也必須判斷您的員工所需的應用程式和功能，以及需要這些應用程式和功能的人員。本文中的資訊可協助您開始使用。

Microsoft Intune 中的應用程式類型

Intune 支援各種不同的應用程式類型。每個應用程式類型的可用選項都不同。Intune可讓您新增並指派下列應用程式類型：

類別	如何安裝	更新
來自市集的應用程式 (市集應用程式)	Intune 在裝置上安裝應用程式。	應用程式更新是自動的。
內部撰寫的應用程式或自訂應用程式 (企業營運)	Intune 在裝置上安裝應用程式 (您提供安裝檔案)。	您必須更新應用程式。
內建 (內建應用程式的應用程式)	Intune 在裝置上安裝應用程式。	應用程式更新是自動的。
網頁上的應用程式 (網頁連結)	Intune 會在裝置主畫面上建立 Web 應用程式的捷徑。	應用程式更新是自動的。
來自其他 Microsoft 服務的應用程式	Intune 會在公司入口網站中建立應用程式的捷徑。如需詳細資訊，請參閱 應用程式來源設定選項 。	應用程式更新是自動的。

特定應用程式類型詳細資料

下表列出特定的應用程式類型，以及如何在 Intune [新增應用程式] 窗格中將其新增：

類別	如何安裝	更新
Android 市集應用程式	市集應用程式	選取 [Android] 作為 平台 ，然後輸入應用程式的 Google Play 商店 URL。
Android 企業版系統應用程式	市集應用程式	選取 [Android] 作為 平台 ，然後輸入應用程式的受控 Google Play 商店 URL。 ¹
iOS/iPadOS 市集應用程式	市集應用程式	選 iOS 作為 平台 、搜尋應用程式，然後在 [Intune] 中選取應用程式。
Microsoft Store 應用程式	市集應用程式	選 Windows 作為應用程式類型，然後輸入應用程式的 Microsoft Store URL。

應用程式類型	平台	說明
受管理的 Google Play 應用程式	市集應用程式	選 [Google Play] 作為 [Google Play] 、搜尋應用程式，然後選取Intune中的應用程式。
適用於 Windows 10 的 Microsoft 365 Apps	市集應用程式 (Microsoft 365)	選 [Microsoft 365 Apps] 底下的 [Windows 10] 作為 [Windows 10] ，然後選取您要安裝的 Microsoft 365 應用程式。
適用於 macOS 的 Microsoft 365 Apps	市集應用程式 (Microsoft 365)	選取 [Microsoft 365 Apps] 底下的 [macOS] 作為 [macOS] ，然後選取 [Microsoft 365 應用程式套件] 。
適用於 Windows 10 的 Microsoft Edge 版本 77 和更新版本	市集應用程式	選 Windows 10 Microsoft Edge 77 底下的 [Microsoft Edge 77] 。
適用於 macOS 的 Microsoft Edge 版本 77 和更新版本	市集應用程式	選取 [Microsoft Edge] 下方的 [macOS**] 77 版和更新版本** 作為 [Microsoft Edge 77] 。
Android 企業營運 (LOB) 應用程式	LOB 應用程式	選 [Android 應用程式] 作為 [Android 應用程式] ，選取 [Android 應用程式] ，然後輸入擴展 [.apk] 的 Android 安裝檔案。
iOS/iPadOS LOB 應用程式	LOB 應用程式	選 [iOS/iPadOS 應用程式] 作為 [iOS/iPadOS 應用程式] ，選取 [iOS/iPadOS 應用程式] ，然後輸入副檔名為 [.ipa] 的 iOS/iPadOS 安裝檔案。
Windows LOB 應用程式	LOB 應用程式	選 [Windows 應用程式] 作為應用程式類型，選取 [Windows 應用程式] ，然後輸入擴展 [.msi] 、 [.appx] 、 [.appxbundle] 、 [.msix] 和 [.msixbundle] 的 Windows 安裝檔案。
內建 iOS/iPadOS 應用程式	內建應用程式	選 [iOS/iPadOS 應用程式] 作為 [iOS/iPadOS 應用程式] ，然後在提供的應用程式清單中選取內建應用程式。
內建 Android 應用程式	內建應用程式	選 [Android 應用程式] 作為 [Android 應用程式] ，然後在提供的應用程式清單中選取內建應用程式。
Web 應用程式	Web 應用程式	選取 [Web 應用程式]** 作為應用程式類型**，然後輸入指向 Web 應用程式的有效 URL。
iOS/iPadOS 網頁剪輯	Web 應用程式	選 [iOS/iPadOS Web 應用程式] 作為 [iOS/iPadOS Web 應用程式] ，然後輸入指向 Web 應用程式的有效 URL。請注意，此應用程式類型僅適用於 iOS/iPadOS 平臺。
Windows Web 連結	Web 應用程式	選 [Windows Web 應用程式] 作為 [Windows Web 應用程式] ，然後輸入指向 Web 應用程式的有效 URL。請注意，此應用程式類型僅適用於 Windows 平臺。
跨平台 Web 應用程式	Web 應用程式	選取 [Web 應用程式]** 作為應用程式類型**，然後輸入指向 Web 應用程式的有效 URL。

類別	類型	說明
Android 企業版系統應用程式	市集應用程式	選取 [Android Enterprise 名稱] 作為 [名稱]，然後輸入應用程式名稱、發行者和套件檔案。
Windows 應用程式 (Win32)	LOB 應用程式	選 [Windows 名稱 (Win32)] 作為 [名稱]，選取 [檔案]，然後選取擴展 [名稱].intunewin [名稱] 安裝檔案。
macOS LOB 應用程式	LOB 應用程式	選 [名稱] 作為 [名稱]，選取 [檔案]，然後選取擴展 [名稱].intunemac [名稱] 安裝檔案。
macOS 應用程式 (DMG)	LOB 應用程式 (非市集應用程式)	選 [macOS 名稱 (DMG)] 作為應用程式類型，選取 [檔案] 檔案，然後選取擴展名為 .dmg 的安裝檔案。

¹ 如需 Android Enterprise 和 Android 工作設定檔的詳細資訊，請參閱下方 [的瞭解授權應用程式](#)。

您可以 **選 > 取 [所有應用程式新增]**，在 [Microsoft Intune] 中 **新增****應用程式 > [選取應用程式類型]** 窗格隨即顯示，並可讓您選取 [應用程式類型]。

TIP

LOB 應用程式是您從應用程式安裝檔案新增的應用程式。例如，若要安裝 iOS/iPadOS LOB 應用程式，您可以在 [名稱] 窗格中選取 [名稱] 作為 [名稱] 來新增應用程式。然後選取應用程式套件檔案 (副檔名為 .ipa)。這些類型的應用程式通常是在內部撰寫，或是自訂應用程式。

評估應用程式需求

身為 IT 管理員，您不僅會決定群組必須使用的應用程式，也會決定每個群組和子群組所需的功能。針對每個應用程式，您會決定所需的平臺、需要應用程式的使用者群組、要套用這些群組的設定原則，以及要套用的保護原則。例如，針對包括 Android 個人擁有工作設定檔在內的註冊類型，您可能想要部署網頁流覽應用程式，以確保使用者能夠開啟連結。

此外，您必須決定要將焦點放在行動裝置管理 (MDM)，還是只在行動應用程式管理 (MAM) 上。

使用 Intune 以 MDM 管理裝置，在下列狀況下很有用：

- 使用者需要 Wi-Fi 或 VPN 公司連線能力設定檔才能提高生產力。
- 使用者需要一組應用程式以推送到他們的裝置。
- 您的組織必須遵守法規或其他原則，以發出特定的 MDM 控制措施，例如安全性或加密。

使用 Intune 在下列狀況下，使用 MAM 管理應用程式而不管裝置很有用：

- 您想要允許使用者使用自己的裝置 (BYOD)。
- 您想要提供一次性快顯訊息，讓使用者知道 MAM 保護已就緒，而不是持續的裝置層級通知。
- 您想要遵守個人裝置上需要較少管理功能的原則。例如，您想要管理應用程式的公司資料，而不是管理整個裝置的公司資料。

如需詳細資訊，請[比較 MDM 和 MAM](#)。

判斷誰將使用應用程式

當您決定員工需要哪些應用程式時，請考慮各種使用者群組及其使用的各種應用程式。在您新增應用程式後，瞭解這些群組也很有幫助。新增應用程式之後，您會指派可使用應用程式的使用者群組。

首先，您必須根據應用程式所包含資料的敏感度，判斷哪個群組應該能夠存取應用程式。您可能需要在組織內包含或排除特定類型的角色。例如，您的銷售群組可能只需要特定的 LOB 應用程式，而專注于工程、財務、人力資源或法律的人員可能不需要使用 LOB 應用程式。此外，您的銷售群組可能需要額外的資料保護，以及存取其行動裝置上的內部公司服務。您必須判斷此群組如何使用應用程式連線到資源。應用程式存取的資料會存在於雲端或內部部署中嗎？此外，使用者如何使用應用程式連線到資源？

Intune 也支援需要安全存取內部部署資料的用戶端應用程式，例如企業營運應用程式伺服器。您通常會使用 Intune 管理的[憑證](#)來進行存取控制，並結合周邊的標準 VPN 閘道或 Proxy，例如 Azure Active Directory 應用程式 Proxy，來提供這種類型的存取。Intune [App Wrapping Tool](#)和 [App SDK](#)可協助您在企業營運應用程式內包含存取的資料，使其無法將公司資料傳遞給取用者應用程式或服務。

使用 [Intune 部署規劃、設計和實作指南](#)，協助您判斷如何識別組織群組。如需將應用程式指派給群組的相關資訊，請參閱 [使用 Microsoft Intune 將應用程式指派給群組](#)。

判斷解決方案的應用程式類型

您可以從下列應用程式類型中選擇：

- **來自市集的應用程式**：已上傳至 Microsoft Store、iOS/iPadOS 市集或 Android 市集的應用程式是市集應用程式。市集應用程式的提供者會維護並提供應用程式更新。您可以在市集清單中選取應用程式，並使用 Intune 作為使用者可用的應用程式加以新增。
- **內部撰寫的應用程式或自訂應用程式 (企業營運)**：內部建立或作為自訂應用程式的應用程式是企業營運 (LOB) 應用程式。此類型應用程式的功能已針對其中一個 Intune 支援的平台建立，例如 Windows、iOS/iPadOS、macOS 或 Android。您的組織會建立更新，並以個別檔案的形式提供您。您可以使用 Intune 來新增和部署更新，以提供應用程式的更新給使用者。
- **Web 上的應用程式**：Web 應用程式是用戶端伺服器應用程式。伺服器提供 Web 應用程式，其中包含 UI、內容和功能。此外，新式網頁裝載平台通常提供安全性、負載平衡和其他優點。此類型的應用程式會在網頁上個別維護。您可以使用 Intune 來指向此應用程式類型。您也可以指派哪些使用者群組可以存取應用程式。
- **來自其他 Microsoft 服務的應用程式**：來自 Azure AD 或 Office Online 的應用程式。Azure AD Enterprise 應用程式 會透過 [Microsoft 端點管理員 系統管理中心](#) 進行註冊和指派。Office Online 應用程式 會使用 [M365 管理員中心](#) 提供的授權控制來指派。您可以對公司入口網站中的使用者隱藏或顯示 Azure AD 企業版和 Office Online 應用程式。從 [Microsoft 端點管理員 系統管理中心](#)，選取 [租使用者系統管理 > 自訂] 以尋找此組態設定。針對每個使用者，選取 [隱藏] 或 [在公司入口網站中顯示 Azure AD 企業 應用程式或 Office Online 應用程式]。每個使用者都會從所選的 Microsoft 服務看到其整個應用程式目錄。根據預設，每個額外的應用程式來源都會設定為 [隱藏]。如需詳細資訊，請參閱 [應用程式來源設定選項](#)。

當您決定組織需要哪些應用程式時，請考慮應用程式如何與雲端服務整合、應用程式存取的資料、應用程式是否可供 BYOD 使用者使用，以及應用程式是否需要網際網路存取。

如需組織所需應用程式類型的詳細資訊，請 [參閱建立設計](#)。

瞭解應用程式管理和保護原則

Intune 可讓您修改所部署應用程式的功能，以協助它們與公司的合規性和安全性原則一致。此控制項可讓您判斷公司資料的受保護方式。Intune 受控應用程式會使用一組豐富的行動應用程式保護原則來啟用，例如：

- 限制複製和貼上和另存新檔函式。
- 設定要在 Microsoft Edge 應用程式內開啟的 Web 連結。
- 啟用多重身分識別使用和應用層級條件式存取。

Intune 管理的應用程式也可以啟用應用程式保護，而不需要註冊，這可讓您選擇套用資料外泄防護原則，而不需要管理使用者的裝置。此外，您可以使用 Intune App SDK 和 App Wrapping Tool，將行動應用程式管理併入您的行動應用程式和企業營運應用程式。如需這些工具的詳細資訊，請參閱 [Intune App SDK 概觀](#)。

瞭解授權的應用程式

除了瞭解 Web 應用程式、市集應用程式和 LOB 應用程式之外，您也應該留意大量採購方案應用程式和授權應用程式的目的，例如：

- **商務用 Apple 大量採購方案 (iOS)** : iOS/iPadOS App Store可讓您為想要在公司中執行的應用程式購買多個授權。購買多個複本可協助您有效率地管理公司中的應用程式。如需詳細資訊, 請 [參閱管理 iOS/iPadOS 大量採購的應用程式](#)。
- **Android Enterprise 完全受控工作設定檔** : 將應用程式指派給 Android Enterprise 完全受控工作設定檔裝置的方式, 與指派給標準 Android 裝置的方式不同。您為 Android Enterprise 完全受控工作設定檔安裝的所有應用程式都來自受控 Google Play 商店。您可以使用Intune來流覽您要的應用程式並核准它們。應用程式接著會出現在入口網站的 [[授權應用程式](#)] 節點中, 而且您可以像管理任何其他應用程式一樣管理應用程式的指派。
- **商務用 Microsoft Store (Windows 10)** : 商務用 Microsoft Store可讓您個別或大量尋找及購買貴組織的應用程式。藉由將市集連線至 Microsoft Intune, 您可以在入口網站中管理大量採購的應用程式。如需詳細資訊, 請[參閱從 商務用 Microsoft Store 管理應用程式](#)。

NOTE

Windows 應用程式的副檔名包括 .msi、.appx、.appxbundle、.msix 和 .msixbundle。

新增應用程式之前

開始新增和指派應用程式之前, 請考慮下列幾點:

- 當您從市集新增和指派應用程式時, 您的使用者必須擁有具有該市集的帳戶, 才能安裝應用程式。
- 您指派的某些應用程式或專案可能取決於內建的 iOS/iPadOS 應用程式。例如, 如果您在 iOS/iPadOS 市集中指派書籍, 裝置上就必須有 iBooks 應用程式。如果您已移除 iBooks 內建應用程式, 就無法使用Intune來恢復它。

IMPORTANT

如果您在部署並安裝應用程式之後, 透過Intune變更應用程式的名稱, 應用程式將無法再使用命令作為目標。

雲端儲存空間

您使用軟體安裝程式安裝類型建立的所有應用程式 (例如, 企業營運應用程式) 會封裝並上傳至Intune雲端儲存體。Intune的試用訂閱帳戶包含 2 GB (GB 的雲端式儲存體), 用來儲存受控應用程式和更新。完整訂閱帳戶不會限制總儲存空間量。

雲端儲存空間的需求如下:

- 所有應用程式安裝檔案都必須位於相同的資料夾中。
- 您上傳之任何檔案的檔案大小上限為 8 GB。

NOTE

Windows 企業營運 (LOB) 應用程式, 包括 Win32、Windows 通用 AppX、Windows 通用 AppX 套件組合、Windows 通用 MSI X 和 Windows 通用 MSI X 套件組合, 每個應用程式的大小上限為 8 GB。所有其他 LOB 應用程式, 包括 iOS/iPadOS LOB 應用程式, 每個應用程式的大小上限為 2 GB。

建立和編輯應用程式的類別

應用程式類別可以用來協助您排序應用程式, 讓使用者更容易在公司入口網站中找到它們。您可以將一或多個類別指派給應用程式, 例如開發 [人員應用程式](#) 或 [通訊應用程式](#)。

當您將應用程式新增至Intune時，您可以選擇選取您想要的類別。使用平台特定的主題來新增應用程式並指派類別。若要建立和編輯您自己的類別，請使用下列程式：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 > 應用程式類別]。
[應用程式類別] 窗格會顯示目前類別的清單。
3. 執行下列其中一項：
 - 若要新增類別，請在 [建立類別] 窗格中選取 [新增]，然後輸入類別的名稱。
名稱只能以一種語言輸入，而且不會由Intune翻譯。
 - 若要編輯類別，請選取類別旁邊 (...) 省略號，然後選取 [釘選到儀表板] 或 [刪除]。
4. 選取 [建立]。

Intune自動新增的應用程式

先前，Intune包含一些您可以快速指派的內建應用程式。根據Intune客戶意見反應，我們移除了這份清單，不再顯示內建應用程式。不過，如果您已指派任何內建應用程式，應用程式仍會顯示在應用程式清單中。您可以視需要繼續指派應用程式。

NOTE

若要安裝必要的非企業營運應用程式，Intune會在裝置簽入時傳送安裝命令來嘗試安裝應用程式，因為未偵測到應用程式，且應用程式的安裝狀態不是 *安裝擱置中*。

安裝、更新或移除必要的應用程式

Intune會在 24 小時內自動重新安裝、更新或移除必要的應用程式，而不是等待 7 天的重新評估週期。

Intune會根據下列條件自動重新安裝、更新或移除必要的應用程式：

- 如果終端使用者卸載您必須在使用者裝置上安裝的應用程式，Intune會在此排程經過時自動重新安裝應用程式。
- 如果必要的應用程式安裝失敗，或是應用程式不在裝置上，Intune評估合規性，並在經過此排程時重新安裝應用程式。
- 系統管理員以使用者群組可用的應用程式為目標，而終端使用者則會從裝置上的公司入口網站安裝應用程式。稍後，系統管理員會將應用程式從 v1 更新為 v2。Intune會在經過此排程時更新應用程式，前提是裝置上仍存在任何舊版的應用程式。
- 如果系統管理員部署卸載意圖，且應用程式存在於裝置上且無法卸載，Intune會評估合規性，並在經過此排程時卸載應用程式。

NOTE

使用 Windows 公司入口網站，如果進度似乎已停止或凍結，使用者可以重新開機應用程式安裝。如果應用程式安裝進度在兩小時內未變更，則允許這項功能。

從 Windows 公司入口網站或公司入口網站網站的 [已 

卸載應用程式

當您需要從使用者的裝置卸載應用程式時，請使用下列步驟。

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 >][所有應用程式 >][應用程式 > 指派][> 新增群組]。

3. 在 [**新增群組**] 窗格中, 選取 [**卸載**]。
4. 選取 [**包含的群組**] 以選取受此應用程式指派影響的使用者群組。
5. 選取您要套用卸載指派的群組。
6. 按一下 [**選取群組**] 窗格上的 [**選取**]。
7. 按一下 [**指派**] 窗格上的 [**確定**] 以設定指派。
8. 如果您想要排除任何使用者群組不受此應用程式指派影響, 請選取 [**排除群組**]。
9. 如果您已選擇排除任何群組, 請在 [**選取群組**] 中選取 [**選取**]。
10. 在 [**新增群組**] 窗格中選取 [**確定**]。
11. 在 [**應用程式指派**] 窗格中選取 [**儲存**]。

IMPORTANT

若要成功卸載應用程式, 請務必先移除要安裝的成員或群組指派, 再將它們指派給卸載。如果將群組指派給安裝應用程式和卸載應用程式, 則應用程式會保留且不會移除。

應用程式安裝錯誤

如需Intune應用程式安裝錯誤的詳細資訊, 請參閱[應用程式安裝錯誤](#)。

後續步驟

若要了解如何將不同平台的應用程式新增至 Intune, 請參閱：

- [Android 市集應用程式](#)
- [Android LOB 應用程式](#)
- [iOS 市集應用程式](#)
- [iOS LOB 應用程式](#)
- [macOS LOB 應用程式](#)
- [Web 應用程式 \(適用於所有平台\)](#)
- [Microsoft Store 應用程式](#)
- [Windows LOB 應用程式](#)
- [適用於 Windows 10 的 Microsoft 365 Apps](#)
- [適用於 macOS 的 Microsoft 365 Apps](#)
- [受管理的 Google Play 應用程式](#)
- [適用於 Windows 10 的 Microsoft Edge](#)
- [適用於 macOS 的 Microsoft Edge](#)
- [內建應用程式](#)
- [Android Enterprise 系統應用程式](#)
- [Win32 應用程式](#)

受 Microsoft Intune 保護的應用程式

2022/9/27 •

此主題中列出的應用程式為支援合作夥伴，以及通常搭配 Microsoft Intune 使用的 Microsoft 應用程式。Intune 受保護的應用程式能以一套豐富的行動應用程式保護原則來啟用。

NOTE

針對您的用戶端企業營運應用程式，您可以使用 [Intune 應用程式軟體開發套件 \(SDK\)](#)，或是 [iOS 版 App Wrapping Tool](#) 和 [Android 版 App Wrapping Tool](#)，來合併行動裝置應用程式管理。

下表提供所支援合作夥伴和通常與 Microsoft Intune 搭配使用之 Microsoft 應用程式的詳細資料。這些應用程式支援 **核心應用程式保護原則** 設定，其定義如下：

- 保護公司或學校帳戶資料，同時在支援多重身分識別的應用程式中保持個人資料不變
- 限制資料傳輸和複製與貼上功能
- 加密公司或學校帳戶資料
- 設定要在受控瀏覽器 (例如 Microsoft Edge) 內部開啟的公司或學校帳戶網頁連結
- 強制實行存取公司或學校帳戶資料的存取權限需求
- 強制實行條件式啟動行為，以保護公司或學校帳戶資料
- 無須管理使用者的裝置，即可套用資料遺失防護原則
- 無須要求註冊，即可啟用應用程式保護
- 在使用協力廠商統一端點管理解決方案進行管理的裝置上，啟用應用程式保護

除了支援核心應用程式保護原則設定外，應用程式也支援 **進階應用程式保護原則** 和 **應用程式組態原則** 設定。這些設定需要應用程式投資：

- 應用程式可使用應用程式組態原則，自訂應用程式行為和 (或) 應用程式保護原則設定。
- 在註冊的裝置上，受控應用程式可以利用「組織允許的帳戶模式」來要求使用特定身分識別登入，以及停用多重身分識別功能。
- 應用程式可使用「同步受原則管理的應用程式資料與原生應用程式」應用程式保護原則設定，限制將連絡人或行事曆資料同步到原生應用程式。
- 應用程式可使用「組織資料通知」應用程式保護原則設定，限制在通知中公開敏感性資料。
- 應用程式可使用「將資料作為組織文件開啟」應用程式保護原則設定，限制匯入來自未受控位置的資料。
- 應用程式可使用「儲存組織資料複本」應用程式保護原則設定，限制在儲存公司或學校帳戶資料時可使用的位址。

Microsoft 應用程式

NOTE

如需條件式存取支援的詳細資訊，請參閱 [應用程式保護原則需求](#)。

下列應用程式支援核心 Intune 應用程式保護原則設定，此外也支援進階應用程式保護原則和應用程式組態原則設定：

名稱	平台	支援情況	備註	Android (iOS ANDROID)	Android (iOS ANDROID)	Android (iOS ANDROID)	Android (iOS ANDROID)	Android (iOS ANDROID)
Microsoft Edge	Android	✓	✓ 參閱 Edge 應用程式設定	✓	不適用	不適用	不適用	不適用
Microsoft Edge	iOS	✓	✓ 參閱 Edge 應用程式設定	✓	不適用	不適用	不適用	不適用
Microsoft Excel	Android	✓	無設定	✓	不適用	✗	✗	✓
Microsoft Excel	iOS	✓	無設定	✓	不適用	✗	✗	✓
Microsoft Launcher	Android	✓	✓ 參閱 啟動程式應用程式設定	✗	不適用	✗	✗	不適用
Microsoft Lens - PDF 掃描器	Android	✗	無設定	✗	不適用	✗	✗	不適用
Microsoft Lens - PDF 掃描器	iOS	✗	無設定	✗	不適用	✗	✗	不適用
Microsoft 清單	iOS	✓	無設定	✓	不適用	不適用	✓	✓
Microsoft 清單	Android	✗	無設定	✗	不適用	不適用	✗	✗
Microsoft Office	Android	✓	✓ 參閱 Office 應用程式設定	✓	不適用	✗	✗	✓
Microsoft Office	iOS	✓	✓ 參閱 Office 應用程式設定	✓	不適用	✗	✗	✓
Microsoft OneDrive	Android	✓	無設定	✓	不適用	✗	✓	不適用
Microsoft OneDrive	iOS	✓	無設定	✓	不適用	✗	✓	不適用

應用程式	平台	支援	設定	支援 (iOS 和 Android)	支援 (iOS 和 Android)	支援 (iOS 和 Android)	支援 (iOS 和 Android)	支援 (iOS 和 Android)
Microsoft OneNote	Android	✓	無設定	✓	不適用	✗	✗	不適用
Microsoft OneNote	iOS	✓	無設定	✓	不適用	✗	✗	不適用
Microsoft Outlook	Android	✓	✓ 參閱 Outlook 應用程式設定	✓	✓	✓	✓	✗
Microsoft Outlook	iOS	✓	✓ 參閱 Outlook 應用程式設定	✓	✓	✓	✓	✓
Microsoft Planner	Android	✓	無設定	✗	不適用	✗	✗	不適用
Microsoft Planner	iOS	✓	無設定	✗	不適用	✗	✗	不適用
Microsoft PowerPoint	Android	✓	無設定	✓	不適用	✗	✗	✓
Microsoft PowerPoint	iOS	✓	無設定	✓	不適用	✗	✗	✓
Microsoft SharePoint	Android	✓	無設定	✗	不適用	✗	✗	不適用
Microsoft SharePoint	iOS	✓	無設定	✗	不適用	✗	✗	不適用
Microsoft Teams	Android	✓	無設定	✓	不適用	✓	✓	✓
Microsoft Teams	iOS	✓	無設定	✓	不適用	✓	✓	✓
Microsoft To-Do	Android	✓	無設定	✗	不適用	✗	✗	不適用
Microsoft To-Do	iOS	✓	無設定	✗	不適用	✗	✗	不適用
Microsoft Word	Android	✓	無設定	✓	不適用	✗	✗	✓

應用程式	平台	支援	設定	支援 (iOS 和 Android)	支援 (iOS 和 Android)	支援 (iOS 和 Android)	支援 (iOS 和 Android)	支援 (iOS 和 Android)
Microsoft Word	iOS	✓	無設定	✓	不適用	✗	✗	✓
Microsoft Yammer	Android	✓	無設定	✗	不適用	✗	✗	不適用
Microsoft Yammer	iOS	✓	無設定	✗	不適用	✗	✗	不適用

下列應用程式支援核心 Intune 應用程式保護原則設定。

應用程式	平台	支援	設定
Dynamics 365 Remote Assist	Android	✓	無設定
Dynamics 365 Remote Assist	iOS	✓	無設定
Dynamics 365 銷售	Android	✓	無設定
Dynamics 365 銷售	iOS	✓	無設定
適用於手機的 Dynamics 365	iOS	✓	無設定
適用於手機的 Dynamics 365	Android	✓	無設定
現場服務 (Dynamics 365)	Android	✓	無設定
現場服務 (Dynamics 365)	iOS	✓	無設定
現場服務行動裝置	Android	✓	無設定
現場服務行動裝置	iOS	✓	無設定
Microsoft 365 系統管理員	Android	✓	無設定
Microsoft 365 系統管理員	iOS	✓	無設定
Microsoft Azure 資訊保護檢視器	Android	✓	無設定
Microsoft Azure 資訊保護檢視器	iOS	✓	無設定
Microsoft Bookings	Android	✓	無設定
Microsoft Bookings	iOS	✓	無設定

應用程式	平台	Intune 支援	保護原則
Microsoft Dynamics CRM	Android	✓	無設定
Microsoft Dynamics CRM	iOS	✓	無設定
Microsoft Kaizala	Android	✓	無設定
Microsoft Kaizala	iOS	✓	無設定
Microsoft PowerApps	Android	✓	無設定
Microsoft PowerApps	iOS	✓	無設定
Microsoft Power Automate	Android	✓	無設定
Microsoft Power Automate	iOS	✓	無設定
Microsoft Power BI	Android	✓	無設定
Microsoft Power BI	iOS	✓	無設定
Microsoft 商務用 Skype	Android	✓	無設定
Microsoft 商務用 Skype	iOS	✓	無設定
Microsoft Stream	Android	✓	無設定
Microsoft Stream	iOS	✓	無設定
Microsoft Visio 檢視器	iOS	✓	無設定
Microsoft Whiteboard	iOS	✓	無設定
Microsoft Whiteboard	Android	✓	無設定

NOTE

若為 Android 版 Microsoft Office，請將 Office Hub、Office Hub (HL) 以及 Office Hub (ROW) 應用程式新增至 Android 應用程式保護原則。

合作夥伴生產力應用程式

下列應用程式支援核心 Intune 應用程式防護原則設定。應用程式也支援進階應用程式保護原則，以及應用程式組態原則設定。如需詳細資訊，請連絡應用程式廠商。

IMPORTANT

如需 Intune 相關支援的特定詳細資料，請與應用程式廠商聯繫。

IIII II	IIIIII	IIIIII APP STORE II
Breezy for Intune 	Breezy For Intune provides secure print capabilities for your iOS device. Our integration with Intune ensures that your data stays secure while on-device, and own our end-to-end encryption and enterprise grade security ensure that it stays that way on its way to the printer.	App Store 連結 (iOS)
CAPTOR 印機 for Intune 	組織會使用 CAPTOR 安全地擷取 iOS/iPadOS 和 Android 裝置上的內容,特別是在醫療保健、法律、政府、執法、保險、房地產、製造和金融服務等管制產業中。CAPTOR 結合了文件掃描、音訊/視訊錄製、相片/文件註解和 QR-Code 讀取的生產力功能。CAPTOR 需要 Inkscreen 的授權金鑰。 主要功能： ● 使用智慧邊緣偵測掃描多頁文件, 以及編輯、標註和儲存為 PDF 的功能。 ● 結合/合併 PDF 檔案, 並重新排列或刪除頁面。 ● 使用 e-Signature 註解簽署 PDF 文件。 ● 擷取高解析度相片和影片。 ● 錄製環境音訊。 ● 讀取 QR 代碼和啟動安全瀏覽器。 ● 使用箭號、繪圖、螢光筆和文字標籤來標註相片和文件。 ● 將資訊輔助字幕套用至媒體。 ● 使用語音辨識來增強包含文字、音訊和視訊的相片和文件搜尋。 ● 設定 IT 原則以強制執行驗證、PDF 版本、開啟於、預設瀏覽器、檔案命名等更多功能。 ● 支援 BYOD/COPE (將工作內容與個人完全分開), 並啟用個人隱私權。	Google Play 連結 (Android), App Store 連結 (iOS)

F2 Manager Intune 	F2 Manager 提供合併的行事曆和清單檢視, 以檢視會議及其相關項目。F2 Manager 支援內嵌註釋和提交處理 (核准程序)。 ■: 若要將 F2 Manager 應用程式與您的商務資料搭配使用, 您必須是 F2 eGovernment 平台的使用者, 且 IT 部門已啟用行動服務。	App Store 連結 (iOS)
F2 Touch Intune 	使用 F2 Touch 應用程式, 您可以存取及編輯公司案例及文件資訊。此應用程式可存取 cBrain F2 eGovernment 平台, 並可讓員工和公司管理工作, 在離開辦公室時安全地執行日常工作。 F2 Touch 應用程式的主要功能: • 管理您的收件匣 • 讀取和核准提交 • 讀取和建立事件及文件 • 聊天 • 搜尋公司文件封存 ■: 若要將 F2 Touch Intune 應用程式與您的商務資料搭配使用, 您必須是 F2 eGovernment 平台的使用者, 且由 IT 部門啟用行動服務和 Intune。	Google Play 連結 (Android), App Store 連結 (iOS)
FactSet 3.0 	FactSet 提供卓越的分析、服務、內容與技術, 協助投資專業人員更快看到並抓住商機。我們的 Factset 3.0 應用程式是一個手機最佳化體驗, 可讓我們的訂閱使用者隨時隨地都能利用 FactSet 工作站的強大功能與情報。	Google Play 連結 (Android), App Store 連結 (iOS)
FleetSafer 	FleetSafer 是一種風險度量及風險降低工具, 可強制執行通訊原則及監控安全駕駛做法。FleetSafer 需要 Cogosense 企業帳戶。FleetSafer 會使用 GPS 或連線的 cogoB 智慧裝置, 在偵測到駕駛動作時自動進行互動, 停用裝置的存取權並停用所有的呼叫和通知。通話、文字、社交和電子郵件功能已停用。駕駛行為受到監視。	Google Play 連結 (Android), App Store 連結 (iOS)
Fuze Mobile for Intune 	適用於 Intune 的 Fuze Mobile 可讓使用者使用語音通話、視訊會議、連絡人中心、聊天訊息和內容共用來進行通訊。系統管理員可以安全地部署 Fuze 行動裝置, 並在 BYOD 內容中大規模擴充。適用於 Intune 的 Fuze Mobile 需要 Fuze 帳戶和 由 Microsoft 管理的環境。	Google Play 連結 (Android), App Store 連結 (iOS)

EEEE EE	EEEEEE	EEEEEE APP STORE EE
iAnnotate for Intune/O365 	專為 Microsoft Intune 企業使用者而設計的適用於 Intune/O365 的 iAnnotate, 可讓您閱讀、標註和共用 PDF、Microsoft Office 檔案、圖像和網頁。與 OneDrive 和 Outlook 無縫整合, 同時將所有 MS 文件輕鬆轉換為可快速標記的 PDF。IT 管理員必須造訪 https://enterprise.iannotate.com/ 以啟用 30 天免費試用版, 並檢視《適用於 Intune 的 iAnnotate 部署指南》。	App Store 連結 (iOS)
iBabs for Intune 	ISEC7 Mobile Exchange Delegate 可讓使用 iPhone 與 iPad 的授權代表同意其同事的約會、管理其連絡人, 以及代表其他使用者回覆電子郵件。	App Store 連結 (iOS)
iManage Work 10 For Intune 	透過使用適用於 Intune 的 Work Mobility, 自信且安全地存取 iManage Work 的內容。讓使用者能夠在其 iOS 裝置中尋找、編輯、共同作業及共用文件和電子郵件。iManage Mobility 可讓使用者在任何地方都有生產力, 擁有一致的使用者經驗, 以及與 iManage Work 10 相同的安全性保護。	App Store 連結 (iOS)
ISEC7 MED for Intune 	ISEC7 Mobile Exchange Delegate 提供行動裝置存取已授權的 Microsoft® Exchange 信箱和公用資料夾。	Google Play 連結 (Android) , App Store 連結 (iOS)
Leap Work for Intune 	Leap Work 是 B2C 通訊應用程式。員工可呼叫或傳送文字、語音及檔案訊息給用戶端所選擇的 Messenger, 例如: WhatsApp、WeChat、Telegram、Line、SMS 及其他。Leap Work 是 LeapXpert 的多通道消息傳送系統 (FMOP) 的一部分。FMOP 概念允許將郵件提升至正式的商務通道, 類似通話或電子郵件。 使用 Leap Work 進行下列作業: • 與客戶在 Messenger 上聯繫 • 擁有並控制所有公司的通訊資料 • 在單一平台上收集員工及客戶通訊 • 允許員工和客戶之間的群組聊天 • 保持公司的通訊歷程記錄隨時待命, 以供監控和合規性之用	Google Play 連結 (Android) , App Store 連結 (iOS)

Lexmark Mobile Print Intune 	行動運算日益普遍，此處於永遠開啟狀態且無障礙的連線可娛樂、啟發並協助完成更多工作。 雖然企業用戶期望桌面列印與行動列印會同樣便利，但 IT 經理知道由於行動裝置的獨特性，提供順暢的輸出可能會很複雜。由於需要解決多種作業系統之間的連線、安全性和網路挑戰，為使用者提供他們所期望的彈性列印可能會很複雜。 Lexmark 所提供的體驗和創新，可協助您滿足使用者的列印需求，讓他們輕而易舉就能取得 IT 技術。我們利用一組全方位工具和選項來解決您的挑戰，協助您達成更透明、簡單且安全的行動列印體驗。	App Store 連結 (iOS)
LumApps for Intune 	適用於 Intune 的 LumApps 允許 Intune 系統管理員組織和保護「攜帶您自己的裝置 (BYOD)」環境。從 Microsoft 端點管理員系統管理中心，系統管理員可以建立原則來保護公司資料，同時讓員工保持連線。LumApps 平台提供公司新聞、商務工具、基本文件和社交社群。 適用於 Intune 的 LumApps 包含許多功能： - 瀏覽列出的內容，包括公司新聞和目標資訊資料流 - 使用附加檔案檢視詳細內容和註解 - 即時回應內容 - 對文章和留言按讚和回應 - 快速查看所有社群，並追蹤您的最愛 - 檢查您偏好的社群活動 - 使用附加的檔案、連結及標籤建立您自己的社群文章 - 快速存取 LumApps 說明頁面 若要使用適用於 Intune 的 LumApps，您公司的使用中 LumApps 訂閱計畫必須包含具有有效登入認證的行動裝置選項。此外，適用於 Intune 的 LumApps 需要 Microsoft 受管理的環境。如果您對使用適用於 Intune 的 LumApps 有問題或疑問，請與貴公司的 IT 管理員聯繫。	Google Play 連結 (Android), App Store 連結 (iOS)

Icon	Icon	Icon APP STORE
Notate for Intune 	Notate 是終極的交換資訊管理員。達成無紙化並改善共同作業。讓 Notate 協助加快您的數位轉型速度。	App Store 連結 (iOS)
Now Mobile - Intune 	員工現在可以跨 IT、人力資源、設施、財務、法務與其他部門尋找答案並完成工作, 這一切都可以從 Now Platform[®] 支援的現代化行動裝置應用程式完成。Now Platform[®] 透過跨部門、系統與人員的數位工作流程, 為員工提供經驗並提高其生產力。 您可以在應用程式中執行的動作範例: • IT: 要求膝上型電腦或重設密碼 • 功能: 尋找及預訂會議室 • 財務: 要求公司信用卡 • 法律資訊: 讓新的供應商簽署保密合約(NDA) • HR: 尋找下一個公司假日並檢查假期原則 由 Now Platform[®] 提供支援的 Now[®] Mobile - 工作生活終於可以像實際生活一樣棒了	Google Play 連結 (Android), App Store 連結 (iOS)
Omnipresence Go 	Omnipresence 是生命科學公司的客戶體驗管理平台。您可以使用 Omnipresence CXM 與生命科學公司的客戶和病人互動。 Omnipresence 是由生命科學專家所組成, 該專家瞭解 pharma、biotech 和 med-裝置的商務需求和合規性需求。在統一平台中, 功能團隊可以使用其顧客的共用檢視和跨裝置的計畫、線上及離線計畫, 與 Microsoft 應用程式的協調地共同運作。透過使用 Omnipresence, 您可以將重點放在透過進階分析和 AI 來提供深入解析, 以豐富客戶旅程的每個階段, 提供卓越客戶體驗。	Google Play 連結 (Android), App Store 連結 (iOS)
PenPoint 	PenPoint 會與 PenLink 的內部部署軟體 PLX 搭配運作, 以進行法律通訊監視作業, 以支援執法調查。適用於 Intune 的 PenPoint 提供安全行動存取, 可存取由 PLX 系統收集及儲存的通訊監控資料。	Google Play 連結 (Android), App Store 連結 (iOS)
PrinterOn for Microsoft 	PrinterOn 的無線行動列印解決方案可讓使用者隨時隨地透過安全網路進行遠端列印。	Google Play 連結 (Android)

Qlik Sense Mobile 	Qlik Sense 是一種市場領先的新一代應用程式，適用於自助導向的分析。Qlik 的專利技術可讓使用者輕鬆地結合來自許多不同來源的資料並自由探索，而不會有查詢型工具的限制。	Google Play 連結 (Android)、 App Store 連結 (iOS)
Re:Work Enterprise 	Re:Work Enterprise 是使用 ActiveSync 的電子郵件用戶端應用程式，是安全、安全且方便的電子郵件用戶端。功能包括與同事共同作業的共用信箱和行事曆。Re:Work Enterprise 支援 Microsoft Exchange Server 和 Microsoft Office365，以及 Microsoft Exchange 電子郵件、行事曆、連絡人、工作和筆記。	Google Play 連結 (Android)、 App Store 連結 (iOS)
RICOH Spaces 	RICOH Spaces 是雲端裝載的工作場所增強平臺，其設計目的是讓您的業務優化，包括桌面預約、空間預約、尋找方式、工作場所深入解析等等。	Google Play 連結 (Android)、 App Store 連結 (iOS)
RingCentral for Intune 	RingCentral for Intune在一個簡單的應用程式中為使用者提供訊息、視訊和電話語音，同時允許 IT 系統管理員強制執行細微的安全性控制來保護公司資料。	Google Play 連結 (Android)、 App Store 連結 (iOS)
SAP Fiori 	藉由使用適用於 iPhone 和 iPad 的 SAP Fiori 用戶端行動應用程式來隨時隨地追蹤最常見的商務工作，提升您每天的生產力。使用這個適用於超過 750 個 SAP Fiori 應用程式 Web 版本的增強型行動執行階段，來提供具有增強型附件處理和全螢幕操作功能的下一層級行動體驗。此外，還能存取客戶以 SAP Fiori 行動服務建置並已可支援 Intune 行動應用程式管理的自訂 SAP Fiori 行動應用程式。	App Store 連結 (iOS)

Secure Contacts 	應用程式 Secure Contacts 可讓您以符合規範的方式，從各種公司資料來源同步處理 iOS 裝置上的商務連絡人。 功能： - 存取所有商務連絡人 - 個人 Microsoft Exchange Online 通訊錄 - 公司通訊錄 - 進一步的資料來源 (Microsoft Dynamics CRM、Salesforce 等) - 我的最愛清單，包括最重要的連絡人 - 未與裝置通訊錄同步處理的來電顯示 - 透過 Microsoft Teams 和 iPhone 的原生應用程式，啟動通話、聊天、簡訊 - 所有資料的加密和相容儲存空間 - 透過 Microsoft Intune (應用程式保護原則) 的行動應用程式管理 - 透過 Azure AD 條件式存取 (相容裝置和應用程式防護原則) 的存取控制 要求： - 需要 Provectus Technologies GmbH 的啟用，才能使用完整功能。 - 若要使用應用程式，Secure Contacts Microsoft Azure AD使用者帳戶必須存在並使用下列功能啟動： - Azure Active Directory Premium P1 (或更新版本) - Exchange Online P1 (或更新版本) - Microsoft Intune - 若要使用 Microsoft Teams 整合功能，必須啟用 Microsoft Teams 功能	App Store 連結 (iOS)
Senses 	Senses 是雲端銷售支援工具。Senses 會協助管理銷售和客戶成功，並建議以累計客戶資訊為基礎的最佳作法。	App Store 連結 (iOS)

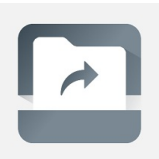
ServiceNow Agent - Intune 	ServiceNow Mobile Agent 應用程式可為最常見的服務台專員工作流程提供現成的行動優先體驗，讓專員能隨時隨地輕鬆進行分級、採取動作，以及解決問題。應用程式可讓服務台專員從他們的行動裝置快速管理及解決終端使用者的問題。專員會使用應用程式的直覺介面來接受及更新工作，即使沒有網際網路連線亦然。應用程式利用原生裝置功能進行導覽、條碼掃描或收集簽名等工作，大幅簡化工作。 應用程式隨附現成的工作流程，可供 IT、客戶服務、人力資源、現場服務、安全性作業與 IT 資產管理中的服務台專員使用。組織可以輕鬆地設定及擴充工作流程，以符合自己的獨特需求。 使用 Mobile Agent，您可以： • 管理指派給您小組的工作。 • 分級事件與案例。 • 使用撥動手勢與快速動作來根據核准執行動作。 • 離線時完成工作。 • 存取完整的問題詳細資料、活動資料流與相關的記錄清單。 • 使用位置、相機與觸控式螢幕硬體將工作流程最佳化	Google Play 連結 (Android), App Store 連結 (iOS)
ServiceNow Onboarding - Intune 	ServiceNow[®] Mobile Onboarding 可讓新進員工完成工作、檢視內容，以及取得跨部門 (包括 IT、人力資源、設施、財務與法務) 的協助，全都從單一原生行動裝置應用程式開始。 讓新進員工能夠執行下列動作，以簡化上線體驗： • 向 IT 訂購膝上型電腦與手機。 • 使用 [設施] 設定工作區。 • 簽署來自法務部門的保密合約 (NDA)。 • 向人力資源部門提交相片並更新個人設定檔。 • 檢閱財務的支出原則，並在有問題時取得協助。 由 Now Platform[®] 提供支援的 Mobile Onboarding 可管理跨多個部門與系統的工作流程，並隱藏後端程序的複雜性。新進員工甚至不需要知道哪些部門牽涉到任何指定流程。他們會收到簡單輕鬆的上線體驗，並可在工作開始之前完成工作，以確保其第一天工作順利。	Google Play 連結 (Android), App Store 連結 (iOS)

Slack for Intune 	Intune 的寬限時間適用於已啟用 Microsoft Intune 行動應用程式管理 (MAM) 的 Slack 客戶。	Google Play 連結 (Android)、App Store 連結 (iOS)
PK Protect for Intune 	適用於 Intune 的 PK 保護是專為在 Intune 環境中運作的現有 PKWARE 客戶而設計。PK 保護可讓您在旅途中完成工作。它快速、安全又容易使用, 讓您不論在任何地方都能維持高生產力。如果您不確定是否有 PK 保護, 請與貴公司的 IT 管理員聯繫。使用 PK 保護, 您可以: 使用 Smartkeys 加密及解密檔案、使用 x.509 數位憑證解密封存、建立及管理 Smartkeys、使用 X.509 數位憑證執行資料的數位簽署及驗證、使用具有強式複雜密碼加密及解密檔案, 包括 AE2、使用現有的 Active Directory 認證登入, 以及建立及查看未加密的 zip 封存。PK 會保護其核心的防護資料, 清除所有使用中、共用或儲存資料的漏洞。將近 30 年來, PKWARE 將加密及壓縮軟體提供給超過 30,000 個企業客戶與超過 200 個政府機關。適用於 iOS/iPadOS 和 Android。	Google Play 連結 (Android)、App Store 連結 (iOS)
Space Connect 	空間連線會將人員和辦公室空間連結在一起, 讓企業能夠更有效率地自動管理辦公空間。使用行動裝置工作區管理解決方案, 預訂辦公桌、會議室、查看您的行事曆、尋找同事等等。	Google Play 連結 (Android)、App Store 連結 (iOS)
Speaking Email 	在您處於移動狀態時為您讀出電子郵件來節省您的時間。專為在駕駛時安全使用而設計的語音命令和簡單手勢可讓您在移動中進行封存、標幟, 或甚至是回覆。 智慧型內容偵測會略過免責聲明、回覆標頭及電子郵件簽章, 只讀出內容而排除待過濾郵件。 員工可透過 Intune 登入來存取 Microsoft 365 Exchange 電子郵件。	App Store 連結 (iOS)

=====	=====	===== APP STORE =====
Zoom for Intune 	Zoom 是您進行會議、網路研討會、聊天和雲端電話的通訊中樞。用完美的視訊、清晰的音訊，以及從桌上型電腦、行動裝置或會議室的即時螢幕畫面分享啟動或加入會議。	Google Play 連結 (Android) 、 App Store 連結 (iOS)

合作夥伴 UEM 應用程式

下列應用程式可在支援 Intune 應用程式防護原則與合作夥伴整合端點管理 (UEM) 解決方案的應用程式之間啟用共存。這些應用程式支援核心 Intune 應用程式防護原則設定。應用程式也支援進階應用程式保護原則，以及應用程式組態原則設定。如需詳細資訊，請連絡應用程式廠商。

=====	=====	===== APP STORE =====
Blackberry Enterprise BRIDGE 	BlackBerry Enterprise BRIDGE 可讓您從 BlackBerry Dynamics 使用 Intune 受控 Microsoft 應用程式 (例如 Microsoft Word、Microsoft PowerPoint 及 Microsoft Excel) 來安全地檢視、編輯及儲存文件。您可以用電子郵件附件的形式來共用文件，並在 BlackBerry Dynamics 與 Intune 受控行動應用程式之間的文件共用過程中維持資料加密。	Google Play 連結 (Android) 、 App Store 連結 (iOS)
Citrix ShareFile for Intune 	Protect corporate data while accessing and sharing files from ShareFile. It directly integrates with Microsoft Word, Excel, and PowerPoint, to allow access to files from ShareFile without ever leaving your office application.	Google Play 連結 (Android) 、 App Store 連結 (iOS)
Workspace ONE Send 	Workspace ONE Send 可使用 VMware 生產力應用程式，為使用 Microsoft Intune 來管理 Microsoft 365 應用程式的客戶提供無縫接軌的編輯和傳送功能。	Google Play 連結 (Android) 、 App Store 連結 (iOS)

後續步驟

若要了解如何將不同平台的應用程式新增至 Intune，請參閱：

- [Android 市集應用程式](#)
- [Android LOB 應用程式](#)
- [iOS 市集應用程式](#)
- [iOS LOB 應用程式](#)
- [Web 應用程式 \(適用於所有平台\)](#)
- [Microsoft Store 應用程式](#)
- [Windows LOB 應用程式](#)
- [適用於 Windows 10 的 Microsoft 365 Apps](#)

- 適用於 macOS 的 Microsoft 365 Apps
- 內建應用程式
- Win32 應用程式

將 Android 市集應用程式新增至 Microsoft Intune

2022/9/27 •

將應用程式指派給裝置或使用者群組之前，您必須先將應用程式新增至Microsoft Intune。

新增應用程式

您可以執行下列動作，將 Android 市集應用程式新增至入口網站Intune：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 >][所有應用程式 >][新增]。
3. 在 [選取應用程式類型] 窗格的可用 市集應用程式 類型下，選取 [Android 市集應用程式]。
4. 按一下 [選取]。
[新增應用程式] 步驟隨即顯示。
5. 若要設定 Android 應用程式的 應用程式資訊，請流覽至 [Google Play 商店](#)，並搜尋您想要部署的應用程式。顯示應用程式頁面，並記下應用程式詳細資料。
6. 在 [應用程式資訊] 頁面中，新增應用程式詳細資料：
 - **名稱**：輸入要在公司入口網站中顯示的應用程式名稱。請確定您使用的任何應用程式名稱都是唯一的。如果應用程式名稱重複，公司入口網站中的使用者只會顯示一個名稱。
 - **描述**：輸入應用程式的描述。此描述會顯示給公司入口網站中的使用者。
 - **Publisher**：輸入應用程式發行者的名稱。
 - **應用程式存放區 URL**：輸入您要建立之應用程式的應用程式市集 URL。當應用程式的詳細資料顯示在市集集中時，請使用應用程式頁面的 URL。
 - **最低作業系統**：在清單中，選取可安裝應用程式的最早作業系統版本。如果您將應用程式指派給具有舊版作業系統的裝置，則不會安裝該應用程式。
 - **類別**：選擇性地選取一或多個內建應用程式類別或您所建立的類別。這麼做可讓使用者在流覽公司入口網站時更容易找到應用程式。
 - **在公司入口網站中將此顯示為精選應用程式**：選取此選項可在使用者流覽應用程式時，在公司入口網站的主頁面上以醒目提示的方式顯示應用程式套件。適用於以可用意圖部署的應用程式。
 - **資訊 URL**：選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
 - **隱私權 URL**：選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
 - **開發人員**：選擇性地輸入應用程式開發人員的名稱。
 - **擁有者**：選擇性地輸入此應用程式擁有者的名稱，例如 *人力資源部門*。
 - **附注**：選擇性地輸入您想要與此應用程式相關聯的任何附注。
 - **標誌**：選擇性地上傳將與應用程式相關聯的圖示。當使用者流覽公司入口網站時，此圖示會隨應用程式一起顯示。
7. 按一下 [下一步] 以顯示 [範圍標籤] 頁面。
8. 按一下 [選取範圍標籤] 來選擇性地為應用程式新增範圍標籤。如需詳細資訊，請參閱 [針對分散式 IT 使用角色型存取控制 \(RBAC\) 和範圍標籤](#)。
9. 按 [下一步] 以顯示 [指派] 頁面。
10. 選取應用程式的群組指派。如需詳細資訊，請參閱 [新增群組以組織使用者和裝置](#)。
11. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。檢閱您為應用程式輸入的值和設定。
12. 當您完成時，按一下 [建立] 將應用程式新增至Intune。

您所建立應用程式的 [概觀] 刀鋒視窗隨即顯示。

後續步驟

- [將應用程式指派給群組](#)

相關主題

- [使用 Intune 將受控 Google Play 應用程式新增至 Android Enterprise 裝置](#)

將 iOS 儲存應用程式新增至 Microsoft Intune

2022/9/27 •

請使用本文中的資訊，協助您新增 iOS 儲存應用程式 Microsoft Intune。iOS 儲存應用程式是 Intune 安裝在使用者裝置上的應用程式。使用者屬於公司的員工。iOS 儲存應用程式會自動更新。

NOTE

雖然 iOS/iPadOS 裝置的使用者可以移除某些內建的 iOS/iPadOS 應用程式，例如股票和地圖，您無法使用 Intune 重新部署這些應用程式。若使用者刪除這些應用程式，則必須移至應用程式存放區，並手動重新安裝。

開始之前

您可以只使用此方法指派應用程式，但不會在應用程式存放區中有足夠的費用。如果您想要使用 Intune 指派付費應用程式，請考慮使用 [iOS/iPadOS 大量購買程式](#)。

NOTE

當您使用 Microsoft Intune 時，建議您使用 Microsoft Edge 或 Google Chrome 瀏覽器。

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 [應用程式] [> > 新增]。
3. 在 [選取應用程式類型] 窗格的 [可用的 儲存區應用程式 類型] 下，選取 [iOS 儲存應用程式]。
4. 按一下 [選取]。
隨即會顯示 [新增應用程式] 步驟。
5. 選取 [搜尋應用程式存放區]。
6. 在 [搜尋應用程式存放區] 窗格中，選取應用程式存放區的國家/地區地區設定。
7. 在 [搜尋] 方塊中，輸入應用程式的名稱 (或名稱) 部分。
Intune 會搜尋存放區，並傳回相關結果的清單。
8. 在 [結果] 清單中，選取您想要的應用程式，然後選取 [選取]。

[應用程式資訊] 頁面會顯示在 [新增應用程式] 窗格中。如有可能，將會根據您從 store 中選取的應用程式來新增應用程式資訊。
9. 在 [應用程式資訊] 頁面中，新增應用程式詳細資料。根據您所選取的應用程式，此窗格中的某些值可能會自動填入：
 - **名稱**: 輸入要顯示在公司入口網站中的應用程式名稱。請確認您使用的任何應用程式名稱都是唯一的。如果應用程式名稱重複，公司入口網站中只會向使用者顯示一個名稱。
 - **描述**: 輸入應用程式的描述。此描述會向公司入口網站中的使用者顯示。
 - **Publisher**: 輸入應用程式發行者的名稱。
 - **APPSTORE URL**: 輸入您要建立之應用程式的應用程式存放區 URL。
 - **最低作業系統**: 在清單中，選取可安裝應用程式的最早作業系統版本。如果您將應用程式指派給具有舊版作業系統的裝置，將不會安裝此應用程式。
 - **適用的裝置類型**: 在清單中，選取應用程式所使用的裝置。

- **類別：**(選用)選取一個或多個內建應用程式類別或您建立的類別。這樣做可讓使用者在流覽公司入口網站時，尋找應用程式的難度。
- **在公司入口網站中將此專案顯示為特色應用程式：**選取此選項，可在使用者流覽應用程式時，在公司入口網站的主要頁面上醒目顯示應用程式套件。
- **資訊 URL：**(選用)輸入包含此應用程式相關資訊的網站 URL。URL 會向公司入口網站中的使用者顯示。
- **隱私權 URL：**選擇性輸入包含此應用程式隱私權資訊的網站 URL。URL 會向公司入口網站中的使用者顯示。
- **開發人員：**(選用)輸入應用程式開發人員的名稱。只有系統管理員才能看到此欄位，而且使用者看不到此欄位。
- **擁有者：**選擇性地輸入此應用程式擁有者的名稱，例如 *HR 部門*。只有系統管理員才能看到此欄位，而且使用者看不到此欄位。
- **附注：**(選用)輸入您想要與此應用程式產生關聯的任何附注。此欄位只會顯示系統管理員，使用者不會看到此欄位。
- **標誌：**(選用)上傳將與應用程式產生關聯的圖示。當使用者流覽公司入口網站時，會隨應用程式一起顯示此圖示。

10. 按 [下一步] 顯示 [範圍標記] 頁面。

11. 按一下 [選取範圍 標籤] 可選擇性地新增應用程式的範圍標記。如需詳細資訊，請參閱 [使用以角色為基礎的存取控制 \(RBAC\) 和範圍標記，以進行發佈](#)。

12. 按 [下一步] 顯示 [工作分派] 頁面。

13. 選取應用程式的群組指派。如需詳細資訊，請參閱 [新增群組以組織使用者和裝置](#)。

14. 按 [下一步] 顯示 [回顧 + 建立] 頁面。檢查您為應用程式輸入的值和設定。

15. 完成後，按一下 [建立]，將應用程式新增至 Intune。

隨即會顯示您建立之應用程式的 **概述** 刀片。

後續步驟

- [將應用程式指派給群組](#)

將 Microsoft Store 應用程式新增至 Microsoft Intune

2022/9/27 •

您必須先將應用程式新增至Intune, 才能指派、監視、設定或保護應用程式。

將應用程式新增至 Intune

您可以執行下列動作, 將 Microsoft Store 應用程式新增至 Intune:

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式] > [新增]。
3. 在 [選取應用程式類型] 窗格的 [可用的市集應用程式 類型] 底下, 選取 [Microsoft Store 應用程式]。
4. 按一下 [選取]。[新增應用程式] 步驟隨即顯示。
5. 若要設定 Microsoft 市集應用程式的 **應用程式資訊**, 請流覽至 [Microsoft Store](#), 選取 [開啟市集應用程式], 然後搜尋您要部署的應用程式。顯示應用程式頁面, 並記下應用程式詳細資料。
6. 在 [應用程式資訊] 頁面中, 新增應用程式詳細資料:
 - **名稱**:輸入要在公司入口網站中顯示的應用程式名稱。請確定您使用的任何應用程式名稱都是唯一的。如果應用程式名稱重複, 公司入口網站中的使用者只會顯示一個名稱。
 - **描述**:輸入應用程式的描述。此描述會顯示給公司入口網站中的使用者。
 - **發行者**:輸入應用程式的發行者名稱。
 - **應用程式存放區 URL**:輸入您要建立之應用程式的App Store URL。
若要尋找 Appstore URL, 請使用下列步驟:
 - a. 流覽至 [Microsoft Store](#)。
 - b. 搜尋並選取所需的應用程式。
 - c. 按一下 [端點管理員] 連結以顯示 [Microsoft 端點管理員詳細資料] 對話方塊。
 - d. 複製 Intune 的連結, 並在將應用程式新增至 Intune 時使用該連結作為 Appstore URL。
 - **類別**:選擇性地選取一或多個內建應用程式類別或您所建立的類別。這麼做可讓使用者在流覽公司入口網站時更容易找到應用程式。
 - **在公司入口網站中將此顯示為精選應用程式**:選取此選項可在使用者流覽應用程式時, 在公司入口網站的主頁面上以醒目提示的方式顯示應用程式套件。
 - **資訊 URL**:選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
 - **隱私權 URL**:選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
 - **開發人員**:選擇性地輸入應用程式開發人員的名稱。
 - **擁有者**:選擇性地輸入此應用程式擁有者的名稱, 例如 *人力資源部門*。
 - **附注**:選擇性地輸入您想要與此應用程式相關聯的任何附注。
 - **標誌**:選擇性地上傳將與應用程式相關聯的圖示。當使用者流覽公司入口網站時, 此圖示會隨應用程式一起顯示。
7. 按一下 [下一步] 以顯示 [範圍標籤] 頁面。
8. 按一下 [選取範圍標籤] 來選擇性地為應用程式新增範圍標籤。如需詳細資訊, 請參閱 [針對分散式 IT 使用角色型存取控制 \(RBAC\) 和範圍標籤](#)。
9. 按 [下一步] 以顯示 [指派] 頁面。
10. 選取應用程式的群組指派。如需詳細資訊, 請參閱 [新增群組以組織使用者和裝置](#)。

11. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。檢閱您為應用程式輸入的值和設定。
12. 當您完成時, 按一下 [建立] 將應用程式新增至Intune。

您所建立應用程式的 [概觀] 刀鋒視窗隨即顯示。

您所建立的應用程式會顯示在應用程式清單中, 您可以將它指派給您選取的群組。

IMPORTANT

Microsoft Store 應用程式只能指派給指派類型 ■ [■] 的群組, (使用者從公司入口網站應用程式或網站) 安裝應用程式。

後續步驟

- [將應用程式指派給群組](#)

如何使用 Microsoft Intune 從商務用 Microsoft Store管理大量採購的應用程式

2022/9/27 •

商務用 Microsoft Store提供您一個位置，讓您能夠個別或大量地尋找及購買貴組織的應用程式。藉由將市集連線至 Microsoft Intune，您可以從入口網站管理大量採購的應用程式。例如：

- 您可以使用 Intune 同步處理您已購買 (或從市集免費) 的應用程式清單。
- 同步處理的應用程式會出現在Intune管理主控台中;您可以像指派任何其他應用程式一樣指派這些應用程式。
- 線上和離線授權的應用程式版本都會同步至Intune。應用程式名稱會在入口網站中附加「線上」或「離線」。
- 您可以追蹤可用的授權數目，以及Intune管理主控台中使用的授權數目。
- 如果可用的授權數目不足，Intune封鎖應用程式的指派和安裝。
- Intune會在使用者從 Azure AD 中刪除時，撤銷商務用 Microsoft Store所管理應用程式的應用程式授權。

開始之前

IMPORTANT

商務用 Microsoft Store將於 2023 年第一季淘汰。不過，在 2023 年淘汰之前，系統管理員仍然可以利用連線從其 UEM 解決方案Microsoft Store商務與教育版，將應用程式部署到受控Windows 11裝置。

開始同步處理並從商務用 Microsoft Store指派應用程式之前，請先檢閱下列資訊：

- 將Intune設定為貴組織的行動裝置管理授權單位。
- 您必須在商務用 Microsoft Store上註冊帳戶。
- 一旦您將 Microsoft 商務Microsoft Store帳戶與Intune相關聯之後，就無法在未來變更為不同的帳戶。
- 從市集購買的應用程式無法從Intune手動新增或刪除。它們只能與商務用 Microsoft Store同步處理。
- 您從商務用 Microsoft Store購買的線上和離線授權應用程式都會同步至Intune。然後，您可以將這些應用程式部署到裝置群組或使用群組。
- 線上應用程式安裝是由市集管理。
- 免費的離線應用程式也可以同步至Intune。這些應用程式是由Intune安裝，而不是由市集安裝。
- 若要使用這項功能，裝置必須加入Active Directory 網域服務、加入 Azure AD 或加入工作場所。
- 已註冊的裝置必須使用 1511 版的 Windows 10 或更新版本。

NOTE

線上商務用 Microsoft Store應用程式只能用於使用者內容安裝;也就是說，透過Intune部署時，您需要以使用者群組為目標。裝置授權離線商務用 Microsoft Store應用程式可以安裝在裝置內容中;也就是說，透過Intune部署時，您可以將裝置群組和使用群組設為目標。

NOTE

如果您透過原則或群組原則) 手動停用受管理裝置上 (存取Microsoft Store，線上授權應用程式將無法安裝。

將您的商務用 Microsoft Store帳戶與Intune

在Intune主控台中啟用同步處理之前，您必須先將市集帳戶設定為使用Intune作為管理工具：

1. 請確定您使用您用來登入Intune的相同租使用者帳戶來登入商務用 Microsoft Store。
2. 在商務Microsoft Store中，選擇 [管理] 索引標籤，選取 [設定]，然後選擇 [散發] 索引卷標。
3. 如果您沒有以 行動 裝置管理工具Microsoft Intune，請選擇 [新增管理工具] 以新增 Microsoft Intune。如果您沒有 Microsoft Intune 啟用為行動裝置管理工具，請按一下 [Microsoft Intune] 旁的 [啟用]。請注意，您應該啟用Microsoft Intune，而不是 Microsoft Intune註冊。

NOTE

您先前只能建立一個管理工具的關聯，以指派應用程式與商務用 Microsoft Store。您現在可以將多個管理工具與存放區建立關聯，例如，Intune和Configuration Manager。

您現在可以在 Intune 主控台中繼續並設定同步處理。

設定同步處理

1. 登入 Microsoft 端點管理員系統管理中心。
2. 選取 [租使用者系統管理 > 連接器和權杖 > 商務用 Microsoft Store]。
3. 按一下 [啟用]。
4. 如果您尚未這麼做，請按一下連結以註冊商務用 Microsoft Store，並如先前所述將您的帳戶建立關聯。
5. 從 [語言] 下拉式清單中，選擇入口網站中顯示商務用 Microsoft Store應用程式的語言。不論顯示的語言為何，它們都會在可用時以使用者的語言安裝。
6. 按一下 [同步]，將您從Microsoft Store購買的應用程式放入Intune。

同步處理應用程式

如果您已經將商務用 Microsoft Store帳戶與Intune系統管理員認證建立關聯，您可以使用下列步驟手動同步處理商務用 Microsoft Store應用程式與Intune。

1. 選取 [租使用者系統管理 > 連接器和權杖 > 商務用 Microsoft Store]。
2. 按一下 [同步]，將您從Microsoft Store購買的應用程式放入Intune。

NOTE

目前不支援具有加密應用程式套件的應用程式，且不會同步至Intune。

指派應用程式

您從市集指派應用程式的方式，與指派任何其他Intune應用程式的方式相同。如需詳細資訊，請參閱[如何將應用程式指派給具有Microsoft Intune的群組](#)。

離線應用程式可以以使用者群組、裝置群組或具有使用者和裝置的群組為目標。離線應用程式可以針對裝置上的特定使用者或裝置上的所有使用者安裝。

當您指派商務用 Microsoft Store應用程式時，安裝應用程式的每個使用者都會使用授權。如果您針對指派的應用程式使用所有可用的授權，就無法再指派任何複本。採取下列其中一個動作：

- 從某些裝置卸載應用程式。
- 減少目前指派的範圍，僅以您擁有足夠授權的使用者為目標。
- 從商務用 Microsoft Store購買更多應用程式複本。

移除應用程式

若要移除從商務用 Microsoft Store 同步處理的應用程式，您必須登入商務用 Microsoft Store 並退款應用程式。無論應用程式是否免費，程式都相同。針對免費應用程式，市集會退款 \$0。下列範例顯示免費應用程式的退款。

The screenshot shows the 'Order details' page in the Microsoft Store. The left sidebar contains navigation links: Home, Quotes, Products & services, My organization, Devices, Billing & payments, Order history (selected), Partners, Permissions, Settings, and Support. The main content area displays order information:

Order date	Order #	Status	Purchased by
10/24/18	9749d007-2ddf-48c0-928c-23ced7771ab2	Complete	Tenant Account

Sold to:
Tenant
1 Microsoft Way
Redmond WA 98052

Total items (1)

Item	Publisher	Quantity	Total	Actions
JT2Go Offline	Siemens Product Lifecycle Management Software	Unlimited	\$0.00	...

A 'Refund' button is visible next to the item.

Summary

Items (1):	\$0.00
Tax:	\$0.00
Total:	\$0.00

Feedback

NOTE

移除應用程式在私人市集中的可見度並不會讓Intune同步處理應用程式。您必須將應用程式退款，才能完全移除應用程式。

後續步驟

- 使用 [Microsoft Intune](#) 管理大量採購的應用程式和書籍

使用 Intune 將受控 Google Play 應用程式新增至 Android Enterprise 裝置

2022/9/27 •

受控 Google Play 是 Google 的企業應用程式市集，也是 Android Enterprise 在Intune中的唯一應用程式來源。您可以使用Intune，透過受控 Google Play 針對任何 Android Enterprise 案例協調應用程式部署，（包括個人擁有的工作設定檔、專用、完全受控和公司擁有的工作設定檔註冊）。將受控 Google Play 應用程式新增至Intune的方式，與針對非 Android Enterprise 新增 Android 應用程式的方式不同。市集應用程式、企業營運 (LOB) 應用程式，以及 Web 應用程式會在受控 Google Play 中核准或新增至受控 Google Play，然後同步處理到Intune，使其出現在 [用戶端應用程式] 清單中。一旦它們出現在 [用戶端應用程式] 清單清單中，您就可以像管理任何其他應用程式一樣管理任何受控 Google Play 應用程式的指派。

為了讓您更輕鬆地設定及使用 Android Enterprise 管理，將您的Intune租使用者連線到受控 Google Play 時，Intune會自動將四個常見的 Android Enterprise 相關應用程式新增至 Intune 管理主控台。這四個應用程式如下：

- **Microsoft Intune** - 用於 Android Enterprise 完全受控案例。在裝置註冊程式期間，此應用程式會自動安裝到完全受控的裝置。
- **Microsoft Authenticator** - 如果您使用雙因素驗證，可協助您登入您的帳戶。在裝置註冊程式期間，此應用程式會自動安裝到完全受控的裝置。
- **Intune 公司入口網站** - 用於應用程式保護原則 (APP) 和 Android Enterprise 個人擁有的工作設定檔案例。在裝置註冊程式期間，此應用程式會自動安裝到完全受控的裝置。
- **受控主畫面** - 用於 Android Enterprise 專用的多應用程式 kiosk 案例。IT 系統管理員應該建立指派，以在將用於多應用程式 Kiosk 案例的專用裝置上安裝此應用程式。

NOTE

當使用者註冊其 Android Enterprise 完全受控裝置時，系統會自動安裝Intune 公司入口網站應用程式，而且使用者可能會看到應用程式圖示。如果終端使用者嘗試啟動Intune 公司入口網站應用程式，終端使用者將會重新導向至Microsoft Intune應用程式，而公司入口網站應用程式圖示隨後會隱藏起來。

開始之前

- 請確定您已將Intune租使用者連線至受控 Google Play。如需詳細資訊，請[參閱將您的Intune帳戶連線到受控 Google Play 帳戶](#)。
- 如果您想要註冊個人擁有的工作設定檔裝置，請確定您已設定Intune和 Android 個人擁有的工作設定檔，以便在入口網站的 [裝置註冊] 工作負載中一起運作。如需詳細資訊，請 [參閱註冊 Android 裝置](#)。

NOTE

當您使用Microsoft Intune時，建議您使用 Microsoft Edge 或 Google Chrome 瀏覽器。

受控 Google Play 應用程式類型

受控 Google Play 提供三種類型的應用程式：

- **受控 Google Play 商店應用程式** - 正式推出于 Play Store 中的公用應用程式。在Intune中管理這些應用程式，方法是流覽您想要管理的應用程式、核准這些應用程式，然後將它們同步至Intune。

- **受控 Google Play 私人應用程式** - 這些是由Intune系統管理員發佈至受控 Google Play 的 LOB 應用程式。這些應用程式是私人應用程式，僅適用於您的Intune租使用者。這是使用受控 Google Play 和 Android Enterprise 來管理及部署 LOB 應用程式的方式。
- **受控 Google Play Web 連結** - 具有 IT 系統管理員定義圖示的 Web 連結，可部署到 Android Enterprise 裝置。這些會出現在裝置應用程式清單中的裝置上，就像一般應用程式一樣。

受控 Google Play 商店應用程式

NOTE

Intune中大部分新建立的專案會採用建立者的範圍標籤。Managed Google Play 商店 應用程式的情況並非如此。系統管理員可以指派範圍標籤，以套用至受控 Google Play 連接器窗格上所有新同步的受控 Google Play 應用程式。如需詳細資訊，請參閱[將您的Intune帳戶連線到受控 Google Play 帳戶](#)。

有兩種方式可以使用 Intune 流覽及核准受控 Google Play 市集應用程式：

1. **直接在 Intune 主控台** 中 - 在Intune內裝載的檢視中流覽和核准市集應用程式。這會直接在 Intune 主控台中開啟，而且不需要您使用不同的帳戶重新驗證。
2. **在受控 Google Play 主控台** 中 - 您可以選擇性地直接開啟受控 Google Play 主控台，並在該處核准應用程式。如需詳細資訊，請參閱[使用 Intune 同步處理受控 Google Play 應用程式](#)。這需要使用您用來將Intune租使用者連線到受控 Google Play 的帳戶來進行個別登入。

直接在 Intune 主控台中新增受控 Google Play 商店應用程式

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式] > [新增]。
3. 在 [選取應用程式類型] 窗格的可用 **市集應用程式** 類型下，選取 [受控 Google Play 應用程式]。
4. 按一下 [選取]。受控 Google Play App Store 隨即顯示。

NOTE

您的Intune租使用者帳戶必須連線到您的 Android Enterprise 帳戶，才能流覽受控 Google Play 商店應用程式。如需詳細資訊，請參閱[將您的Intune帳戶連線到受控 Google Play 帳戶](#)。

5. 選取應用程式以檢視應用程式詳細資料。
6. 在顯示應用程式的頁面上，按一下 [核准]。應用程式的視窗隨即開啟，要求您授與應用程式執行各種作業的許可權。
7. 選取 [核准] 以接受應用程式許可權並繼續。
8. 在 [核准設定] 索引標籤中，選取 [應用程式要求新許可權時保持核准]，然後按一下 [完成]。

IMPORTANT

如果您未選擇此選項，如果應用程式開發人員發佈更新，則必須手動核准任何新的許可權。這會導致應用程式的安裝和更新停止，直到許可權獲得核准為止。基於這個理由，建議您選取自動核准新許可權的選項。

9. 按一下 [選取] 以選取應用程式。
10. 按一下刀鋒視窗頂端的 [同步]，以同步處理應用程式與受控 Google Play 服務。
11. 按一下 [重新整理] 以更新應用程式清單，並顯示新增的應用程式。

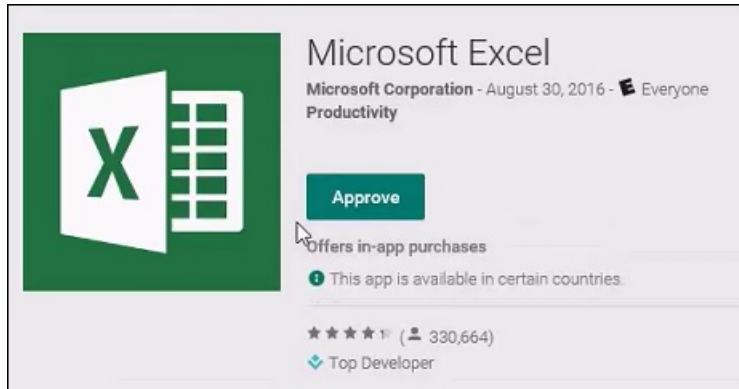
在受控 Google Play 主控台中新增受控 Google Play 商店應用程式 (替代)

如果您想要將受控 Google Play 應用程式與Intune同步，而不是直接使用Intune來新增它，請使用下列步驟。

IMPORTANT

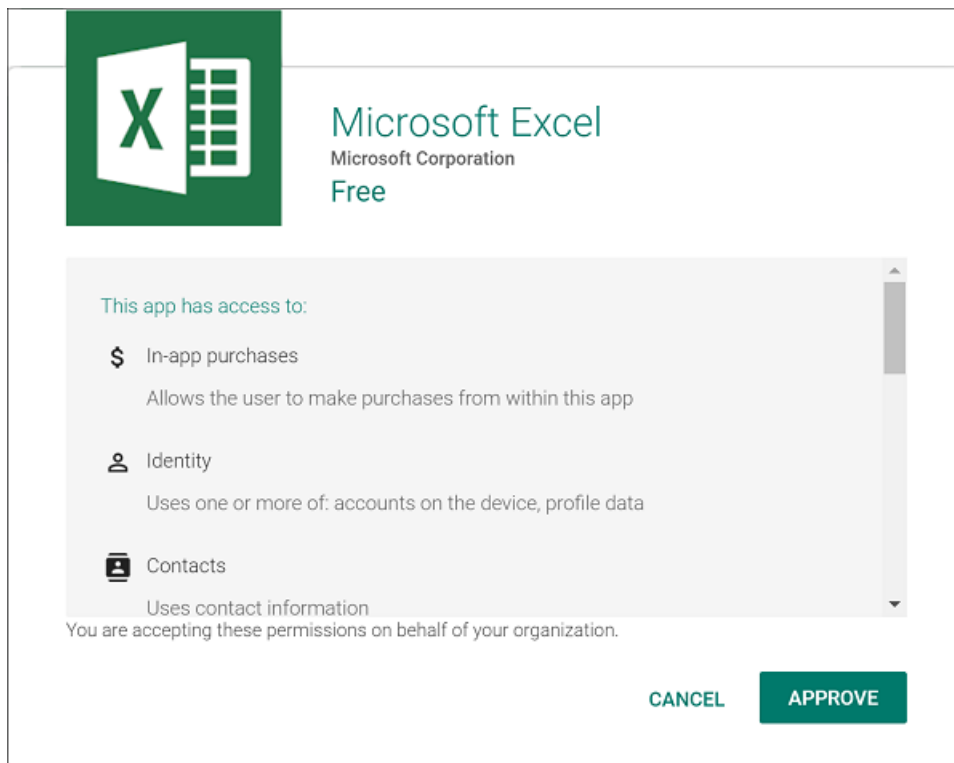
以下提供的資訊是使用 Intune 新增受控 Google Play 應用程式的替代方法，如上所述。

1. 移至受控 Google Play 商店。使用您用來設定 Intune 與 Android Enterprise 之間連線的相同帳戶登入。
2. 搜尋市集，然後使用 Intune 選取您想要指派的應用程式。
3. 在顯示應用程式的頁面上，按一下 [核准]。
在下列範例中，已選擇 Microsoft Excel 應用程式。



應用程式的視窗隨即開啟，要求您授與應用程式執行各種作業的許可權。

4. 選取 [核准] 以接受應用程式許可權並繼續。



5. 選取處理新應用程式許可權要求的選項，然後選取 [儲存]。

APPROVAL SETTINGS

NOTIFICATIONS



Microsoft Excel
Microsoft Corporation

How would you like to handle new app permission requests?

☒ **Keep approved when app requests new permissions.**
Users will be able to install the updated app.

☐ **Revoke app approval when this app requests new permissions.**
App will be removed from the store until it is reapproved.

CANCEL

SAVE

應用程式已核准，且會顯示在您的 IT 管理主控台中。接下來，您可以[使用 Intune 同步處理受控 Google Play 應用程式](#)。

受控 Google Play 私人 (LOB) 應用程式

有兩種方式可將 LOB 應用程式新增至受控 Google Play：

1. 直接在 Intune 主控台中 - 這可讓您直接在 Intune 內提交應用程式 APK 和標題，以新增 LOB 應用程式。此方法不需要您擁有 Google 開發人員帳戶，也不需要支付向 Google 註冊為開發人員的費用。這個方法比較簡單，而且步驟數目大幅減少，而且可讓 LOB 應用程式在 10 分鐘內可供管理。
2. 在 Google Play 開發人員主控台中 - 如果您有 Google 開發人員帳戶，或想要設定僅適用於 Google Play 開發人員主控台的進階散發功能，(如新增其他應用程式螢幕擷取畫面)，您可以使用 [Google Play 開發人員主控台](#)。

受控 **Google Play 私人 (LOB) 應用程式** 直接在 Intune 主控台中發佈

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式] > [新增]。
3. 在 [選取應用程式類型] 窗格的可用 **市集應用程式** 類型下，選取 [受控 Google Play 應用程式]。
4. 按一下 [選取]。受控 Google Play App Store 會顯示在 Intune 內。
5. 選取 [Google Play] 視窗中 **鎖定圖示** 旁邊 (私人應用程式)。
6. 按一下右下方的 [+] 按鈕以新增應用程式。
7. 新增應用程式 標題，然後按一下 [上傳 APK] 新增 APK 應用程式套件。

NOTE

您的應用程式套件名稱在 Google Play 中必須是全域唯一的 (不只是您企業或 Google Play 開發人員帳戶) 中的唯一名稱。否則，您會收到上 **APK 錯誤**。

8. 按一下 [建立]。
9. 如果您已完成新增應用程式，請關閉 [受控 Google Play] 窗格。
10. 按一下 [應用程式] 窗格上的 [同步處理]，以與受控 Google Play 服務同步。

NOTE

私人應用程式可能需要幾分鐘的時間才能進行同步處理。如果應用程式未在第一次執行同步處理時出現，請等候幾分鐘並起始新的同步處理。您也可以從受控 Google Play 商店同步處理應用程式。如需相關資訊，請參閱[使用 Intune 同步處理受控 Google Play 應用程式](#)。

如需受控 Google Play 私人應用程式的詳細資訊，包括常見問題，請參閱 Google 的支援文章：
<https://support.google.com/googleplay/work/answer/9146439>

IMPORTANT

使用此方法新增的私人應用程式永遠無法公開。只有當您確定此應用程式一律是貴組織的私人應用程式時，才使用此發佈選項。

使用 Google 開發人員主控台發佈受控 Google Play 私人 (LOB) 應用程式

1. 使用您用來設定 Intune 與 Android Enterprise 之間連線的相同帳戶登入[Google Play 開發人員主控台](#)。

NOTE

如果您是第一次登入，您必須註冊並支付費用，才能成為 Google 開發人員計畫的成員。

2. 在 主控台中，新增應用程式。如需詳細資訊，請參閱 Google 的支援檔：[發佈私人應用程式](#)。
3. 您上傳和提供應用程式的相關資訊的方式，與將任何應用程式發佈至 Google Play 商店的方式相同。不過，您必須特別使用 Google Play 主控台來新增您的組織。如需詳細資訊，請參閱 Google 的支援檔 [發佈至您自己的組織](#)。

NOTE

請遵循 Google 的支援檔，讓應用程式僅供您的組織使用。應用程式將無法在公用 Google Play 商店上使用。

如需上傳和發佈 Android 應用程式的詳細資訊，請參閱 [Google 開發人員主控台說明](#)。

4. 發佈應用程式之後，請使用您用來設定 Intune 與 Android Enterprise 之間連線的相同帳戶來登入受控[Google Play 商店](#)。
5. 在市集的 [應用程式] 節點中，確認已顯示您已發佈的應用程式。
應用程式會自動核准與Intune同步處理。

受控 Google Play Web 連結

受控 Google Play Web 連結是可安裝且可管理的，就像其他 Android 應用程式一樣。安裝在裝置上時，它們會連同已安裝的其他應用程式一起出現在使用者的應用程式清單中。選取時，它們會在裝置的瀏覽器中啟動。

NOTE

如果您已設定Intune應用程式保護原則設定 [] 為受原則 []，則從受控 Google Play 向下推送的 Web 連結將不會在 Microsoft Edge 的公司內容中開啟。透過受控 Google Play 向下推送 Web 連結時，無法辨識為 MAM 管理的應用程式，這就是為什麼如果使用者未使用個人帳戶登入，Microsoft Edge 會以個人內容或 InPrivate 模式開啟。如需相關資訊，請參閱[Microsoft Intune 中的 Android 應用程式保護原則設定](#)。

Web 連結會以 Microsoft Edge 或您選擇部署的任何其他瀏覽器應用程式開啟。請務必將至少一個瀏覽器應用程式部署到裝置，讓 Web 連結能夠正確開啟。不過，所有適用於網頁連結的 **顯示** 選項 (全螢幕、獨立和最小 UI) 僅

適用於 Chrome 瀏覽器。

若要建立受控 Google Play Web 連結：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式] > [新增]。
3. 在 [選取應用程式類型] 窗格的可用 **市集應用程式** 類型下，選取 [受控 Google Play 應用程式]。
4. 按一下 [選取]。受控 Google Play App Store 會顯示在Intune內。
5. 選取 [Google Play] 視窗中 [地球] 圖示) 旁 (Web 應用程式。
6. 按一下右下方的 [+] 按鈕以新增應用程式。
7. 新增應用程式 標題、Web 應用程式 URL、選取應用程式的顯示方式，然後選取應用程式圖示。
8. 按一下 [建立]。
9. 如果您已完成新增應用程式，請關閉 [受控 Google Play] 窗格。
10. 按一下 [應用程式] 窗格上的 [同步 處理]，以與受控 Google Play 服務同步。

NOTE

Web 應用程式可能需要幾分鐘的時間才能進行同步處理。如果應用程式未在第一次執行同步處理時出現，請等候幾分鐘並起始新的同步處理。

同步處理受控 Google Play 應用程式與Intune

如果您已核准來自市集的應用程式，但未在 **應用程式** 工作負載中看到它，請強制立即同步處理，如下所示：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [租使用者系統管理 > 連接器和權杖 > 受控 Google Play]。
3. 在 [受控 Google Play] 窗格中，選擇 [同步]。
頁面會更新上次同步處理的時間和狀態。
4. 在 Microsoft 端點管理員 系統管理中心內，選取 [所有應用程式 >]。
隨即顯示新可用的受控 Google Play 應用程式。

將受控 Google Play 應用程式指派給 Android Enterprise 個人擁有和公司擁有的工作設定檔裝置

當應用程式顯示在 [應用程式] 工作負載窗格的 [應用程式授權] 節點中時，您可以指 [派它](#)，就像將應用程式指派給使用者群組來指派任何其他應用程式一樣。

指派應用程式之後，它會安裝 (或可在您設為目標之使用者的裝置上安裝)。系統不會要求裝置的使用者核准安裝。如需 Android Enterprise 個人擁有工作設定檔裝置的詳細資訊，請參閱 [設定 Android Enterprise 個人擁有工作設定檔裝置的註冊](#)。

NOTE

只有已指派的應用程式才會顯示在使用者的受控 Google Play 商店中。因此，這是系統管理員在使用受控 Google Play 設定應用程式時所採取的重要步驟。

將受控 Google Play 應用程式指派給 Android Enterprise 完全受控裝置

[Android Enterprise 完全受控裝置](#) 是與單一使用者相關聯的公司擁有裝置，專門用於工作而非個人用途。完全受控裝置上的使用者可以從其裝置上的受控 Google Play 應用程式取得其可用的公司應用程式。

根據預設，Android Enterprise 完全受控裝置不允許員工安裝組織未核准的任何應用程式。此外，員工將無法根據原則移除任何已安裝的應用程式。如果您想要允許使用者存取完整的 Google Play 商店來安裝應用程式，而不是只存取受控 Google Play 商店中核准的應用程式，您可以將 [允許存取 Google Play 商店中的所有應用程式] 設定為 [允許]。透過此設定，使用者可以使用其公司帳戶存取 Google Play 商店中的所有應用程式，不過購買可能會受到限制。您可以允許使用者將新帳戶新增至裝置，以移除有限的購買限制。這麼做可讓終端使用者能夠使用個人帳戶從 Google Play 商店購買應用程式，以及進行應用程式內購買。如需詳細資訊，請參閱[使用 Intune 來允許或限制功能的 Android Enterprise 裝置設定](#)。

NOTE

Microsoft Intune 應用程式、Microsoft Authenticator 應用程式和公司入口網站應用程式將會在上線期間安裝為所有完全受控裝置的必要應用程式。自動安裝這些應用程式可提供條件式存取支援，Microsoft Intune 應用程式使用者可以看到並解決合規性問題。

更新受控 Google Play 應用程式

根據預設，除非符合下列條件，否則受控 Google Play 應用程式不會更新：

- 裝置已連線到 wi-fi
- 裝置正在充電
- 未主動使用裝置
- 要更新的應用程式未在前景執行

如需詳細資訊，請參閱從 Google [管理應用程式更新檔](#)。

您可以在裝置設定原則中設定應用程式自動更新，以選擇設定專用、完全受控和公司擁有之工作設定檔裝置的 Wi-Fi 需求。

針對專用、完全受控和公司擁有的工作設定檔裝置，您可以在應用程式指派給群組時選擇應用程式更新模式。可用的更新模式如下：

- **預設** 值：應用程式的更新受限於上述) 所述 (預設條件。
- **高優先順序**：應用程式會在發行新更新時儘快更新，而忽略所有預設條件。這對某些使用者可能會造成干擾，因為在使用裝置時可能會發生更新。
- **延遲**：當應用程式收到新的更新時，會觸發 90 天的等候期間。90 天后，應用程式會更新為可用的最新版本，即使該版本不是觸發等候期間的更新也一樣。請注意，90 天的視窗無法設定。若要提早結束等候期間，請將更新模式變更為 [預設] 或 [高優先順序]。

若要編輯應用程式更新模式：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式] > [所有應用程式]。
3. 從應用程式清單中選取應用程式。
4. 選取 [內容]。
5. 選取 [指派] 區段的 [編輯]。
6. 按一下該群組的對應群組模式，以尋找您想要編輯應用程式更新模式的群組。
7. 在 [應用程式設定] 底下，選取所需的更新模式。

管理 Android Enterprise 應用程式許可權

Android Enterprise 會要求您先在受控 Google Play Web 主控台中核准應用程式，才能將應用程式與 Intune 同步，

並將其指派給您的使用者。因為 Android Enterprise 可讓您以無訊息方式自動將應用程式推送至使用者的裝置，所以您必須代表所有使用者接受應用程式許可權。使用者在安裝應用程式時看不到任何應用程式許可權，因此請務必瞭解許可權。

當應用程式開發人員使用新版本的應用程式更新許可權時，即使您核准了先前的許可權，也不會自動接受許可權。執行繼承應用程式的裝置仍然可以使用它。不過，在核准新的許可權之前，應用程式不會升級。在您核准應用程式的新許可權之前，未安裝應用程式的裝置不會安裝應用程式。

更新應用程式許可權

定期造訪受控 Google Play 主控台，以檢查是否有新的許可權。您可以設定 Google Play，在核准的應用程式需要新許可權時傳送電子郵件給您或其他人。如果您指派應用程式，並觀察其未安裝在裝置上，請遵循下列步驟檢查是否有新的許可權：

1. 移至 [Google Play](#)。
2. 使用您用來發佈和核准應用程式的 Google 帳戶登入。
3. 選取 [更新] 索引標籤，並檢查是否有任何應用程式需要更新。
任何列出的應用程式都需要新的許可權，而且在套用之前不會被指派。

或者，您可以將 Google Play 設定為根據每個應用程式自動重新布建應用程式許可權。

Android Enterprise 個人擁有工作設定檔裝置的其他受控 Google Play 應用程式報告

針對部署至 Android Enterprise 個人擁有工作設定檔裝置的受控 Google Play 應用程式，您可以使用 Intune 來檢視安裝在裝置上的應用程式狀態和版本號碼。

使用受控 Google Play 封閉式測試播放軌

您可以將受控 Google Play 應用程式的非生產版本散發到在 Android Enterprise 案例中註冊的裝置，(Android Enterprise 個人擁有的工作設定檔 (BYOD)、Android Enterprise 完全受控 (COBO)、使用 Azure AD 共用模式註冊的 Android Enterprise 專用裝置 (也稱為 COSU)，以及 Android Enterprise 公司擁有的工作設定檔 ())，以執行測試。在 Intune 中，您可以查看應用程式是否已發佈生產前組建測試播放軌，以及是否能夠將該追蹤指派給 Azure Active Directory 使用者群組或裝置群組。將生產版本指派給目前存在的群組的工作流程，與指派非生產通道相同。部署之後，每個播放軌的安裝狀態會與受控 Google Play 中的曲目版本號碼對應。如需詳細資訊，請參閱 [Google Play 的關閉測試播放軌，以進行應用程式發行前測試](#)。

NOTE

對於在 Android Enterprise 個人擁有的工作設定檔 (BYOD) 中註冊的裝置，目前不適用非生產應用程式播放軌的必要應用程式部署。

刪除受控 Google Play 應用程式

必要時，您可以從 Microsoft Intune 刪除受控 Google Play 應用程式。若要刪除受控 Google Play 應用程式，請在入口網站中開啟 [Microsoft Intune]，然後選取 [所有應用程式 >]。從應用程式清單中，選取受控 Google Play 應用程式右側的省略號 (...)，然後從顯示的清單中選取 [刪除]。當您從應用程式清單中刪除受控 Google Play 應用程式時，會自動取消核准受控 Google Play 應用程式。

NOTE

如果未核准或從受控 Google Play 商店中刪除應用程式，則不會從Intune用戶端應用程式清單中移除該應用程式。即使未核准應用程式，這仍可讓您將卸載原則的目標設為使用者。

若要關閉 Android Enterprise 註冊和管理，請參閱 [中斷 Android Enterprise 系統管理帳戶的連線](#)。

Android 企業版系統應用程式

您可以為 [Android Enterprise 專用裝置](#) 或 [完全受控裝置](#) 啟用 Android Enterprise 系統應用程式。如需新增 Android Enterprise 系統應用程式的詳細資訊，請參閱 [將 Android Enterprise 系統應用程式新增至 Microsoft Intune](#)。

已向 Azure AD 共用模式註冊 AE 專用裝置的 MAM 原則

Intune Azure AD 共用模式註冊的受控 Android Enterprise 專用裝置可以接收 MAM 原則，而且可以與其他 Android 企業裝置分開設定目標。未處於共用裝置模式的 Intune 受控 Android Enterprise 專用裝置將繼續遭到封鎖，無法取得 MAM。如需使用 Azure AD 共用模式註冊 Intune 受控 Android Enterprise 專用裝置的詳細資訊，請參閱 [Android Enterprise 專用裝置](#)。

後續步驟

- [將應用程式指派給群組](#)

使用 Microsoft Intune 將 Microsoft 365 Apps 新增至 Windows 10/11 裝置

2022/9/27 •

您必須先將應用程式新增至Intune, 才能指派、監視、設定或保護應用程式。其中一個可用的[應用程式類型](#)是適用於Windows 10裝置的 Microsoft 365 應用程式。藉由在Intune中選取此應用程式類型, 您可以將 Microsoft 365 應用程式指派並安裝到您管理的執行Windows 10裝置。如果您擁有應用程式的授權, 您也可以為Microsoft Project Online桌面用戶端和 Microsoft Visio Online 方案 2 指派和安裝應用程式。可用的 Microsoft 365 應用程式會顯示為 Azure 內 Intune 主控台中應用程式清單中的單一專案。

NOTE

Microsoft Office 365 專業增強版已重新命名為 **Microsoft 365 Apps** ■。在我們的檔中, 我們通常會將其稱為 **Microsoft 365 Apps**。

您必須使用 Microsoft 365 App 授權來啟用透過 Microsoft Intune 部署的 Microsoft 365 App 應用程式。Intune 支援使用 microsoft 365 商務版商務用應用程式版, 但是您必須使用 XML 資料設定商務版 Microsoft 365 應用程式版的 app 套件。如需詳細資訊, 請參閱[使用 XML 資料設定應用程式套件](#)。

不支援使用 Office 部署工具 (ODT) 透過 Intune 安裝 OneDrive。不過, OneDrive 會安裝為某些 Microsoft 365 應用程式安裝的元件。如需相關資訊, 請參閱[Office 部署工具](#)的組態選項。

開始之前

IMPORTANT

如果終端使用者裝置上.msi Office 應用程式, 您必須使用 ■ MSI 功能安全地卸載這些應用程式。否則, Intune提供的 Microsoft 365 應用程式將無法安裝。

多個必要或可用的應用程式指派不會加總。稍後的應用程式指派將會覆寫預先存在的已安裝應用程式指派。

- 您部署這些應用程式的裝置必須執行Windows 10 Creators Update或更新版本。
- Intune僅支援從 Microsoft 365 Apps 套件新增 Office 應用程式。
- 如果在Intune安裝應用程式套件時開啟任何 Office 應用程式, 安裝可能會失敗, 而且使用者可能會遺失未儲存檔案的資料。
- Windows 家用版、Windows 團隊版、Windows 全像攝影版或Windows Holographic for Business裝置不支援此安裝方法。
- Intune不支援從 Microsoft Store 安裝 Microsoft 365 傳統型應用程式 (稱為 Office Centennial 應用程式) 在您已使用 Intune 部署 Microsoft 365 應用程式的裝置上。如果您安裝此設定, 可能會造成資料遺失或損毀。
- 多個必要或可用的應用程式指派不會加總。稍後的應用程式指派將會覆寫預先存在的已安裝應用程式指派。例如, 如果第一組 Office 應用程式包含 Word, 而後一組則不包含 Word, 則會卸載 Word。此條件不適用於任何 Visio 或 Project 應用程式。
- 目前不支援多個 Microsoft 365 部署。只有一個部署會傳遞至裝置。
- Office 版本 - 選擇您要指派 32 位或 64 位版本的 Office。您可以在 32 位和 64 位裝置上安裝 32 位版本, 但只能在 64 位裝置上安裝 64 位版本。
- 從使用者裝置移除 MSI - 選擇您是否要移除使用者裝置預先存在的 Office .MSI 應用程式。如果使用者裝置上有預先存在的 .MSI 應用程式, 則安裝不會成功。要卸載的應用程式不限於在設定 App Suite 中選取要安裝的應用程式, 因為它會從使用者裝置移除所有 Office (MSI) 應用程式。如需詳細資訊, 請參閱[升級至](#)

Microsoft 365 Apps 時移除現有的 Office MSI 版本。當Intune使用者的電腦上重新安裝 Office 時，終端使用者會自動取得與先前MSI Office 安裝相同的語言套件。

選取Microsoft 365 Apps

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式] > [新增]。
3. 在 [選取 應用程式類型] 窗格的 [Microsoft 365 Apps] 區段中，選取 [Windows 10]。
4. 按一下 [選取]。[新增Microsoft 365 Apps 步驟隨即顯示]。

步驟 1 - 應用程式套件資訊

在此步驟中，您會提供應用程式套件的相關資訊。此資訊可協助您在Intune中識別應用程式套件，並協助使用者在公司入口網站中尋找應用程式套件。

1. 在 [應用程式套件資訊] 頁面中，您可以確認或修改預設值：
 - **套件名稱**：輸入應用程式套件在公司入口網站中顯示的名稱。請確定您使用的所有套件名稱都是唯一的。如果相同的應用程式套件名稱存在兩次，公司入口網站中只會向使用者顯示其中一個應用程式。
 - **套件描述**：輸入應用程式套件的描述。例如，您可以列出您已選取要包含的應用程式。
 - **發行者**：Microsoft 會顯示為發行者。
 - **類別**：選擇性地選取一或多個內建應用程式類別或您所建立的類別。此設定可讓使用者在流覽公司入口網站時更容易找到應用程式套件。
 - **在公司入口網站中將此顯示為精選應用程式**：選取此選項可在使用者流覽應用程式時，在公司入口網站的主頁面上以醒目提示的方式顯示應用程式套件。
 - **資訊 URL**：選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
 - **隱私權 URL**：選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
 - **開發人員**：Microsoft 會顯示為開發人員。
 - **擁有者**：Microsoft 會顯示為擁有者。
 - **附注**：輸入您想要與此應用程式相關聯的任何附注。
2. 按一下 [下一步] 以顯示 [設定 應用程式套件] 頁面。

步驟 2 - (四 1) 使用設定設計工具設定應用程式套件

您可以選取組態設定 **格式** 來選擇設定應用程式設定的方法。設定格式選項包括：

- 設定設計工具
- 輸入 XML 資料

當您選擇 [設定設計工具] 時，[新增應用程式] 窗格將會變更為提供三個額外的設定區域：

- 設定應用程式套件
- 應用程式套件資訊
- 屬性

Add Microsoft 365 Apps ...

Microsoft 365 Apps (Windows 10)

- 1 App suite information 2 **Configure app suite** 3 Scope tags 4 Assignments 5 Review + create

Configuration settings format *

Configuration designer

Configure app suite

Select Office apps ⓘ

9 selected

Select other Office apps (license required) ⓘ

0 selected

App suite information

These settings apply to all apps you have selected in the suite. [Learn more](#)

Architecture ⓘ

32-bit

64-bit

Update channel * ⓘ

Select one

Remove other versions ⓘ

Yes

No

Version to install ⓘ

Latest

Specific

Specific version

Latest version

Properties

Use shared computer activation ⓘ

Yes

No

Accept the Microsoft Software License Terms on behalf of users

Yes

No

Install background service for Microsoft Search in Bing ⓘ

Yes

No

Languages ⓘ

No languages selected

Previous

Next

1. 在 [設定應用程式套件] 頁面上，選擇 [設定設計工具]。

- **選取 [Office 應用程式]:**選擇下拉式清單中的應用程式，選取您想要指派給裝置的標準 Office 應用程式。
- **選取) 所需的其他 Office 應用程式 (授權:**選擇下拉式清單中的應用程式，選取您想要指派給裝置的其他 Office 應用程式，以及您擁有授權的其他 Office 應用程式。這些應用程式包括授權應用程式，例如Microsoft Project Online桌面用戶端和 Microsoft Visio Online 方案 2。
- **架構:**選擇您要指派 32 位 或 64 位 版本的Microsoft 365 Apps。您可以在 32 位和 64 位裝置上安裝 32 位版本，但只能在 64 位裝置上安裝 64 位版本。
- **更新通道:**選擇在裝置上更新 Office 的方式。如需各種更新通道的相關資訊，請參閱[Microsoft 365 Apps 企業版 的更新通道概觀](#)。從下列專案中選擇：
 - 每月
 - 每月 (目標)
 - 半年

- 半年 (已設定目標)

選擇通道之後，您可以選擇下列專案：

- **移除其他版本**：選擇 [是] 以從使用者裝置移除其他版本的 Office (MSI)。當您想要從使用者裝置移除預先存在的 Office .MSI 應用程式時，請選擇此選項。如果使用者裝置上有預先存在的 .MSI 應用程式，則安裝不會成功。要卸載的應用程式不限於在設定 App Suite 中選取要安裝的應用程式，因為它會從使用者裝置移除所有 Office (MSI) 應用程式。如需詳細資訊，請參閱[升級至 Microsoft 365 Apps 時移除現有的 Office MSI 版本](#)。當Intune使用者的電腦上重新安裝 Office 時，終端使用者會自動取得與先前.MSI Office 安裝相同的語言套件。
- **要安裝的版本**：選擇應安裝的 Office 版本。
- **特定版本**：如果您已選擇 [特定] 作為要在上述設定中 **安裝的版本**，您可以選取在終端使用者裝置上為選取的通道安裝特定版本的 Office。

可用的版本會隨著時間而變更。因此，建立新的部署時，可用的版本可能較新，而且沒有特定的較舊版本可用。目前的部署會繼續部署較舊的版本，但每個通道都會持續更新版本清單。

對於更新其固定版本 (或更新任何其他屬性) 並部署為可用的裝置，如果裝置已安裝舊版，則報告狀態會顯示為 [已安裝]，直到裝置簽入發生為止。發生裝置簽入時，狀態會暫時變更為 [未知]，但不會向使用者顯示。當使用者起始較新可用版本的安裝時，使用者會看到狀態變更為已安裝。

如需詳細資訊，請參閱[Microsoft 365 Apps 更新通道概觀](#)。

- **使用共用電腦啟用**：當多位使用者共用電腦時，請選取此選項。如需詳細資訊，請參閱[共用電腦啟用Microsoft 365 Apps的概觀](#)。
- **自動接受應用程式使用者授權合約**：如果您不需要使用者接受授權合約，請選取此選項。然後Intune會自動接受合約。
- **語言**：Office 會自動安裝在終端使用者裝置上隨 Windows 一起安裝的任何支援語言中。如果您要使用應用程式套件安裝其他語言，請選取此選項。

您可以針對透過 Intune 管理Microsoft 365 Apps部署其他語言。可用語言的清單包含 (核心、部分和校訂) 的語言套件 **類型**。在入口網站中，選取 [Microsoft Intune > 應用程式 > 所有應用程式 > 新增]。在 [新增應用程式] 窗格的 [應用程式類型] 清單中，選取 [Microsoft 365 Apps] 底下的 [Windows 10]。在 [應用程式套件設定] 窗格中選取 [語言]。如需詳細資訊，請參閱在 [Microsoft 365 Apps 中部署語言的概觀](#)。

2. 按一下 [下一步] 以顯示 [範圍標籤] 頁面。

步驟 2 - (四 2) 使用 XML 資料設定應用程式套件

如果您在 [設定 應用程式套 件] 頁面的 [設定格式] 下拉式方塊下選取 [輸入 XML 資料] 選項，您可以使用自訂群組態檔來設定 Office 應用程式套件。

Add Microsoft 365 Apps ...

Microsoft 365 Apps (Windows 10)

- 1 App suite information 2 **Configure app suite** 3 Scope tags 4 Assignments 5 Review + create

Configuration settings format *

Enter XML data

Configuration file

Use the Office Customization tool to create the configuration files that are used to deploy Office in large organizations. [Learn more](#)

```
<Configuration>
  <Add SourcePath="\\Server\Share"
    OfficeClientEdition="32"
    Channel="SemiAnnual" >
    <Product ID="O365ProPlusRetail">
      <Language ID="en-us" />
      <Language ID="ja-jp" />
    </Product>
    <Product ID="VisioProRetail">
      <Language ID="en-us" />
      <Language ID="ja-jp" />
    </Product>
  </Add>
  <Updates Enabled="TRUE"
    UpdatePath="\\Server\Share" />
  <Display Level="None" AcceptEULA="TRUE" />
</Configuration>
```

Validate XML

Previous

Next

1. 已新增組態 XML。

NOTE

產品識別碼可以是商務 (0365BusinessRetail) 或 Proplus (0365ProPlusRetail)。不過, 您只能使用 XML 資料來設定 Microsoft 365 Apps 商務版 版的應用程式套件。請注意, Microsoft Office 365 專業增強版已重新命名為 Microsoft 365 Apps 。

2. 按一下 [下一步] 以顯示 [範圍標籤] 頁面。

如需輸入 XML 資料的詳細資訊, 請參閱 [Office 部署工具的組態選項](#)。

步驟 3 - 選取選用 (範圍標籤)

您可以使用範圍標籤來判斷誰可以在Intune中看到用戶端應用程式資訊。如需範圍標籤的完整詳細資料, 請 [參閱針對分散式 IT 使用角色型存取控制和範圍標籤](#)。

1. 按一下 [選取範圍標籤], 選擇性地新增應用程式套件的範圍標籤。
2. 按 [下一步] 以顯示 [指派] 頁面。

步驟 4 - 指派

1. 選取 [必要]、[適用於已註冊的裝置] 或 [卸載 應用程式套件的群組指派]。如需詳細資訊，請參閱[新增群組以組織使用者和裝置](#)和[使用Microsoft Intune將應用程式指派給群組](#)。
2. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。

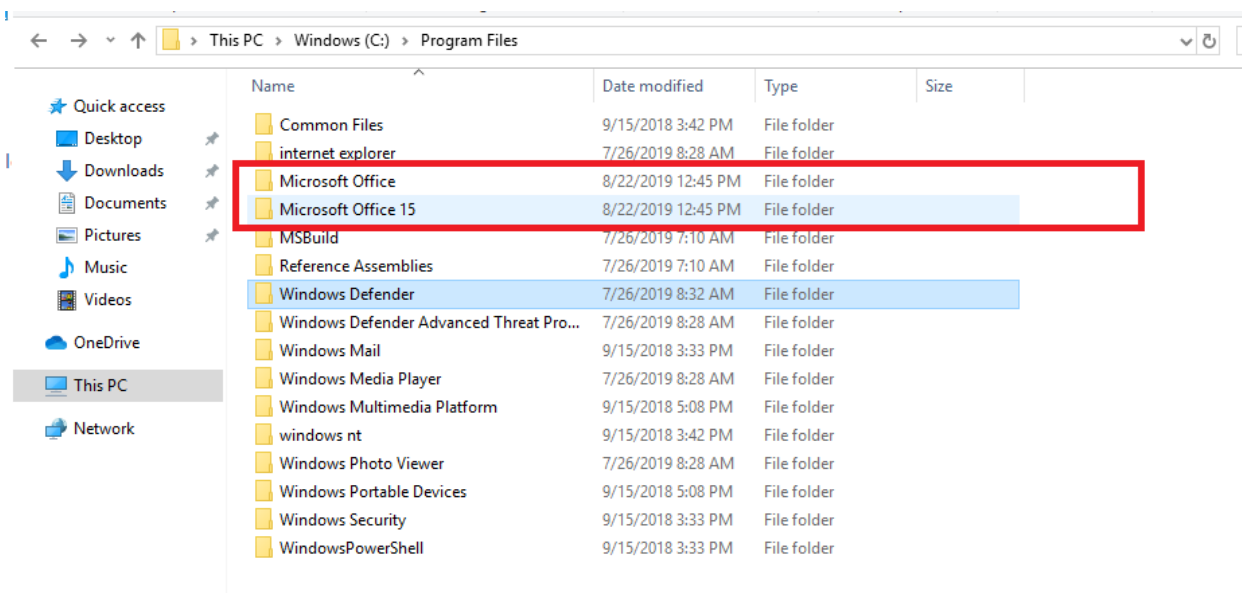
步驟 5 - 檢視 + 建立

1. 檢閱您為應用程式套件輸入的值和設定。
2. 當您完成時，按一下 [建立] 將應用程式新增至Intune。

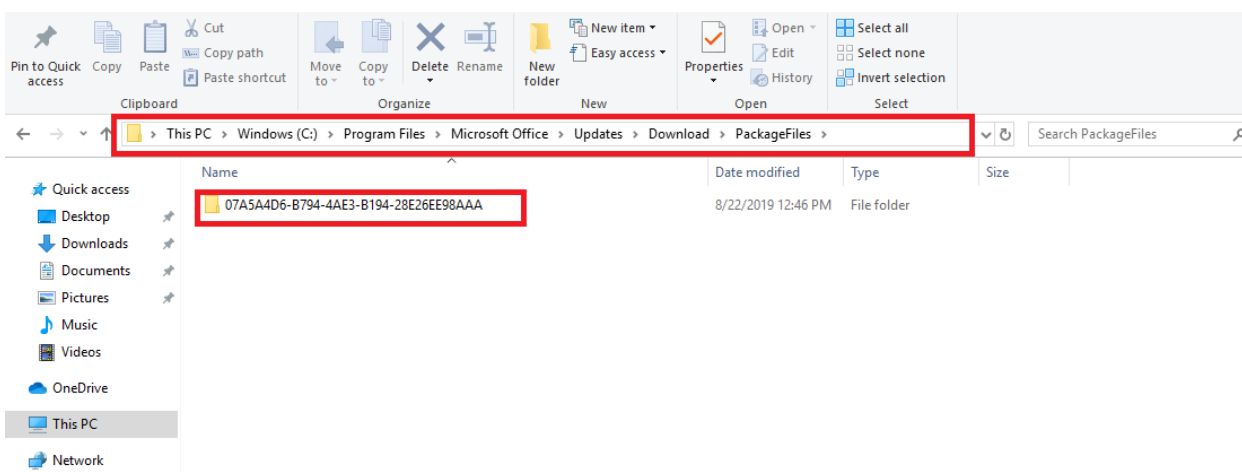
[概觀] 刀鋒視窗隨即顯示。

部署詳細資料

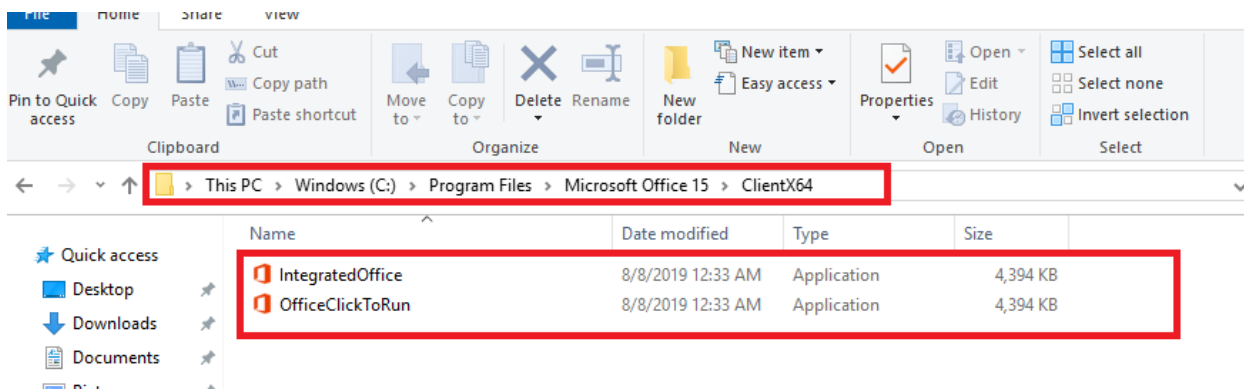
一旦透過 Office 設定服務提供者將來自 Intune 的部署原則指派給目的機器 (CSP)，終端裝置就會自動從 *officecdn.microsoft.com* 位置下載安裝套件。您會看到兩個目錄出現在 *Program Files* 目錄中：



在 *Microsoft Office* 目錄下，會在安裝檔案儲存所在的位置建立新資料夾：



在 *Microsoft Office 15* 目錄下，會儲存 Office 隨選即用安裝啟動器檔案。如果需要指派類型，安裝將會自動啟動：



如果已視需要設定 Microsoft 365 的指派，安裝將會處於無訊息模式。安裝成功後，將會刪除下載的安裝檔案。如果指派設定為 [可用]，則 Office 應用程式會出現在公司入口網站應用程式中，讓使用者可以手動觸發安裝。

疑難排解

Intune使用[Office 部署工具](#)，使用 Office 365 [CDN 將Microsoft 365 Apps](#)下載並部署到您的用戶端電腦。參考[管理Office 365端點](#)中概述的最佳做法，以確保您的網路設定允許用戶端直接存取 CDN，而不是透過中央 Proxy 路由傳送 CDN 流量，以避免產生不必要的延遲。

IMPORTANT

針對自訂 Office 部署工具 XML 安裝，安裝狀態只會反映安裝嘗試的結果。安裝狀態不會反映應用程式目前是否安裝在電腦上。

如果您遇到安裝或執行時間問題，請在目標裝置上執行[適用於 Microsoft 365 的 Microsoft 支援服務](#)和修復小幫手。

其他疑難排解詳細資料

當您無法將 Microsoft 365 應用程式安裝到裝置時，您必須識別問題是否Intune相關或 OS/Office 相關。如果您可以看到 *Microsoft Office* 和 *Microsoft Office 15* 這兩個資料夾出現在裝置的 *Program Files* 目錄中，您可以確認 Intune已成功起始部署。如果您看不到兩個資料夾出現在 [程式檔] 下方，您應該確認下列情況：

- 裝置已正確註冊到Microsoft Intune。
- 裝置上有作用中的網路連線。如果裝置處於飛航模式、已關閉或位於沒有服務的位置，則在建立網路連線之前，將不會套用原則。
- 符合Intune和 Microsoft 365 網路需求，並可根據下列文章存取相關的 IP 範圍：
 - [Intune網路設定需求和頻寬](#)
 - [Office 365 URL 與 IP 位址範圍](#)
- 已將 Microsoft 365 應用程式套件指派給正確的群組。

此外，監視 *目錄 C:\Program Files\Microsoft Office\更新\Download* 的大小。從Intune雲端下載的安裝套件將會儲存在此位置。如果大小不會增加或只是增加非常緩慢，建議您再次檢查網路連線能力和頻寬。

一旦您得出Intune和網路基礎結構都如預期般運作的結論，您應該從作業系統的觀點進一步分析問題。請考慮下列條件：

- 目標裝置必須在Windows 10 Creators Update或更新版本上執行。
- 部署應用程式時，不會開啟任何現有的 Office 應用程式Intune。
- 現有 MSI 版本的 Office 已正確地從裝置中移除。Intune使用與 Office MSI 不相容的 Office 隨選即用。本檔會進一步說明此行為：
[不支援在相同電腦上使用隨選即用和 Windows Installer 安裝的 Office](#)

- 登入使用者應該具有在裝置上安裝應用程式的許可權。
 - 根據 Windows 記錄檔應用程式，確認沒有任何問題事件檢視器 **記錄 > 檔**。
 - 在安裝期間擷取 Office 安裝詳細資訊記錄。如果要執行這項操作，請依照下列步驟執行：
 1. 在目的電腦上啟用 Office 安裝的詳細資訊記錄。若要這樣做，請執行下列命令來修改登錄：


```
reg add HKLM\SOFTWARE\Microsoft\ClickToRun\Override /v LogLevel /t REG_DWORD /d 3
```
 2. 再次將 Microsoft 365 Apps 部署至目標裝置。
 3. 等候大約 15 到 20 分鐘，然後移至 %temp% 資料夾和 %windir%\temp 資料夾，依 **修改日期** 排序，挑選根據重現時間修改的 {Machine Name}-{TimeStamp}.log 檔案。
 4. 執行下列命令以停用詳細資訊記錄：


```
reg delete HKLM\SOFTWARE\Microsoft\ClickToRun\Override /v LogLevel /f
```
- 詳細資訊記錄可以提供安裝程式的進一步詳細資訊。

安裝應用程式套件期間發生錯誤

如需如何檢視詳細資訊安裝記錄的資訊，請參閱[如何啟用 Microsoft 365 Apps ULS 記錄](#)。

下表列出您可能會遇到的常見錯誤碼及其意義。

Office CSP 的狀態

❏	❏	❏
1460 (ERROR_TIMEOUT)	下載	無法下載 Office 部署工具
13 (ERROR_INVALID_DATA)	-	無法驗證已下載 Office 部署工具的簽章
CertVerifyCertificateChainPolicy 的錯誤碼	-	下載的 Office 部署工具的認證檢查失敗
997	Wip	安裝
0	安裝之後	安裝成功
1603 (ERROR_INSTALL_FAILURE)	-	未通過任何必要條件檢查，例如：SxS (嘗試在安裝 2016 MSI 時安裝) 版本不符其他專案
0x8000ffff (E_UNEXPECTED)	-	嘗試在電腦上沒有隨選即用 Office 時卸載
17002	-	無法完成安裝) (案例。可能的原因：userInstallation 在安裝期間因另一個安裝而取消安裝已取消磁碟空間未使用語言識別項
17004	-	未知的 SKU

Office 部署工具錯誤碼

❏	❏❏	UI	❏❏❏
沒有作用中的隨選即用安裝時卸載工作	-2147418113、0x8000ffff 或 2147549183	錯誤碼：30088-1008 錯誤碼：30125-1011 (404)	Office 部署工具

II	III	UI	IIII
安裝 MSI 版本時安裝	1603	-	Office 部署工具
安裝已由使用者或另一個安裝取消	17002	-	隨選即用
嘗試在已安裝 32 位的裝置上安裝 64 位。	1603	-	Office 部署工具傳回碼
嘗試安裝未知的 SKU (不是 Office CSP 的合法使用案例, 因為我們應該只傳入有效的 SKU)	17004	-	隨選即用
空間不足	17002	-	隨選即用
隨選即用用戶端無法啟動 (非預期的)	17000	-	隨選即用
隨選即用用戶端無法排入佇列案例, (非預期的)	17001	-	隨選即用

後續步驟

- 若要將應用程式套件指派給其他群組，請參閱 [將應用程式指派給群組](#)。

使用 Microsoft Intune 指派 macOS 裝置的 Microsoft 365

2022/9/27 •

這種應用程式類型可讓您輕鬆地將 Microsoft 365 應用程式指派給 macOS 裝置。使用此應用程式類型，您可以安裝 Word、Excel、PowerPoint、Outlook、OneNote、Teams 和 OneDrive。為了協助讓應用程式更安全且最新，應用程式隨附于 Microsoft AutoUpdate (MAU)。您想要的應用程式會在 Intune 主控台內的應用程式清單中顯示為一個應用程式。

NOTE

其他的 Mac 版 Office 版本可以新增至 Microsoft 端點管理員系統管理中心。如需詳細資訊，請參閱[大多數目前的 Mac 版 Office 封裝](#)。

Microsoft Office 365 專業增強版已重新命名為 **Microsoft 365 Apps**。在我們的檔中，我們通常會將其稱為 **Microsoft 365 Apps**。

開始之前

在您開始將 Microsoft 365 應用程式新增至 macOS 裝置之前，請先瞭解下列詳細資料：

- 您部署這些應用程式的裝置必須執行 macOS 10.14 或更新版本。
- 當 Intune 安裝應用程式套件時，如果有任何 Office 的應用程式已開啟，使用者可能會遺失未儲存檔案的資料。

選取 Microsoft 365 Apps

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用 > > 程式][新增]。
3. 在 [選取應用程式類型] 窗格的 [Microsoft 365 Apps] 區段中，選取 macOS。
4. d. 按一下 [選取]。隨即會顯示 [新增 Microsoft 365 Apps] 步驟。

步驟 1-應用程式套件資訊

在這個步驟中，您會提供應用程式套件的相關資訊。此資訊可協助您識別 Intune 中的應用程式套件，以及協助使用者在公司入口網站中尋找應用程式套件。

1. 在 [應用程式套件資訊] 頁面中，您可以確認或修改預設值：
 - **套件名稱**：輸入應用程式套件的名稱，因為它會顯示在公司入口網站中。請確定您使用的所有套件名稱都是唯一的。如果相同的應用程式套件名稱都存在兩次，則只有其中一個應用程式會向公司入口網站中的使用者顯示。
 - **套件描述**：輸入應用程式套件的描述。例如，您可以列出您已選取要包含的應用程式。
 - **Publisher**：Microsoft 會顯示為發行者。
 - **類別**：(選用)選取一個或多個內建的應用程式類別或您建立的類別。此設定可讓使用者在流覽公司入口網站時，尋找應用程式套件會比較容易。
 - **在公司入口網站中將此專案顯示為特色應用程式**：選取此選項，可在使用者流覽應用程式時，在公司入口網站的主要頁面上醒目顯示應用程式套件。
 - **資訊 URL**：(選用)輸入包含此應用程式相關資訊的網站 URL。URL 會向公司入口網站中的使用者顯

示。

- **隱私權 URL**：選擇性輸入包含此應用程式隱私權資訊的網站 URL。URL 會向公司入口網站中的使用者顯示。
- **開發人員**：Microsoft 出現為開發人員。
- **擁有者**：Microsoft 會顯示為擁有者。
- **附注**：輸入您想要與此應用程式產生關聯的任何附注。
- **標誌**：當使用者流覽公司入口網站時，會顯示應用程式的 Microsoft 365 Apps 標誌。

2. 按一下 [下一步] 以顯示 [範圍標籤] 頁面。

步驟 2-選取範圍標記 (選用)

您可以使用範圍標記，判斷誰可以在 Intune 中查看用戶端應用程式資訊。如需範圍標籤的完整詳細資料，請參閱 [使用角色型存取控制和範圍標籤來發佈它](#)。

1. 按一下 [選取範圍 標籤] 可選擇性地新增應用程式套件的範圍標記。
2. 按 [下一步] 顯示 [工作分派] 頁面。

步驟 3-工作分派

1. 為應用程式套件的 [已註冊的裝置] 群組指派選取 [必要] 或 [可用]。如需詳細資訊，請參閱使用 Microsoft Intune, [新增群組以組織使用者和裝置](#)，並 [指派應用程式至群組](#)。

NOTE

您無法透過 Intune 卸載「Microsoft 365 macOS」應用程式套件的應用程式。

2. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。

步驟 4-審閱 + 建立

1. 檢查您為應用程式套件輸入的值和設定。
2. 完成後，按一下 [建立]，將應用程式新增至 Intune。

顯示 [一覽] 刀片式伺服器。套件會以單一專案的方式出現在應用程式清單中。

後續步驟

- 若要瞭解如何將 Microsoft 365 應用程式新增至 Windows 10 裝置，請參閱 [使用 Microsoft Intune 將 Microsoft 365 Apps 指派給 Windows 10 裝置](#)。
- 若要深入瞭解從使用者群組中包含或排除應用程式指派，請參閱 [納入和排除應用程式指派](#)。

在 Microsoft Intune 中管理 Android Enterprise 系統應用程式

2022/9/27 •

將 Android Enterprise 系統應用程式指派給裝置之前，您必須先在 Microsoft Intune 中啟用應用程式。Android Enterprise 裝置上支援系統應用程式。您可以為 [Android Enterprise 專用裝置](#)、[完全受控裝置](#)、[Android Enterprise 公司擁有的工作設定檔](#) 或 [Android Enterprise 個人擁有的工作設定檔](#) 啟用系統應用程式。當您不再需要系統應用程式時，可以停用它。Android Enterprise 系統應用程式將會啟用或停用已屬於平臺一部分的應用程式。若要啟用應用程式，請將系統應用程式指派為 **必要**。若要停用應用程式，請將系統應用程式指派為 **[卸載]**。系統應用程式無法指派為可供使用者使用。

在 Intune 中啟用系統應用程式

您可以使用下列步驟，在 Intune 中啟用 Android Enterprise 系統應用程式：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 **[所有 > 應用程式] > [新增]**。
3. 在 **[選取應用程式類型]** 窗格的 **[可用的其他 類型]** 底下，選取 **[Android Enterprise 系統應用程式]**。
4. 按一下 **[選取]**。**[新增應用程式]** 步驟隨即顯示。在 **[應用程式資訊]** 頁面中，新增應用程式詳細資料：
 - **應用程式名稱**：輸入應用程式的名稱。
 - **發行者**：輸入應用程式的發行者名稱。
 - **套件名稱**：輸入套件名稱。Intune 會驗證封裝名稱是否有效。
5. 按一下 **[下一步]** 以顯示 **[範圍標籤]** 頁面。
6. 按一下 **[選取範圍標籤]** 來選擇性地為應用程式新增範圍標籤。如需詳細資訊，請參閱 [針對分散式 IT 使用角色型存取控制 \(RBAC\) 和範圍標籤](#)。
7. 按 **[下一步]** 以顯示 **[指派]** 頁面。
8. 選取應用程式的群組指派。若要啟用應用程式，請將應用程式指派為 **必要**。如需詳細資訊，請參閱 [新增群組以組織使用者和裝置](#)。
9. 按一下 **[下一步]** 以顯示 **[檢視 + 建立]** 頁面。檢閱您為應用程式輸入的值和設定。
10. 當您完成時，按一下 **[建立]** 以在 Intune 中啟用應用程式。

您所建立應用程式的 **[概觀]** 刀鋒視窗隨即顯示。

NOTE

您必須使用裝置的 OEM 來尋找您想要啟用/停用之應用程式的套件名稱。

當受控 Google Play 在 Intune 中有相同的應用程式時，您就無法建立 Android Enterprise 系統應用程式。

您所建立的應用程式會顯示在應用程式清單中，您可以將它指派給您選取的群組。

在 Intune 中停用系統應用程式

您可以使用下列步驟，在 Intune 中停用 Android Enterprise 系統應用程式：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 **[應用程式] > [所有應用程式]**。
3. 從應用程式清單中選取系統應用程式。

4. 將此應用程式的指派變更為 **[卸載 並儲存]**。

後續步驟

- [將應用程式指派給群組](#)

將 web 應用程式新增至 Microsoft Intune

2022/9/27 •

Intune 支援各種應用程式類型，包含 web 應用程式。Web 應用程式是用戶端伺服器應用程式。伺服器提供 web 應用程式，其中包含 UI、內容及功能。此外，現代網頁主控平臺一般會提供安全性、負載平衡及其他優點。Web 應用程式會在網頁上分開維護。您可以使用 Microsoft Intune 指向此應用程式類型。您也可以指派可存取此應用程式的使用者群組。

在您為使用者管理及指派應用程式之前，請將 app 新增至 Intune。

Intune 會在使用者的裝置上建立 web 應用程式的快捷方式。若為 iOS/iPadOS 裝置，web app 的快捷方式會新增至主畫面。針對 Android 裝置系統管理裝置，會將 web 應用程式的快捷方式新增至 Intune 公司入口網站小工具，且該小工具必須由使用者手動鎖定。Windows 裝置上，web app 的快捷方式會置於 [開始] 功能表上。

NOTE

瀏覽器必須安裝在使用者的裝置上，才可啟動 web 應用程式。

若為 Android Enterprise 裝置，請參閱[Managed Google Play web 連結](#)。

在 iOS 裝置中，(固定 web 應用程式的新網頁剪貼網站) 會在需要時于 Microsoft Edge 中開啟以在受保護的瀏覽器中開啟，而不是 Intune Managed Browser。若為舊版的 iOS 網頁剪貼網站，您必須重新取得這些網頁剪貼網站的目標，以確保它們在 Microsoft Edge 中開啟，而不是受管理的流覽

若為舊版裝置系統管理員 Android 裝置，則只有在使用者的公司入口網站版本比 5.0.4737.0 舊的情況下，才能使用 Intune Managed Browser 來開啟透過公司入口網站構件釘住的網頁連結。

將 web 應用程式新增至 Intune

若要將應用程式新增至 Intune 以作為網頁上之應用程式的快捷方式，請執行下列操作：

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 [應用程式] [> > 新增]。
3. 在 [選取應用程式類型] 窗格的 [可用的 其他 類型] 下，選取 [Web 連結]。
4. 按一下 [選取]。隨即會顯示 [新增應用程式] 步驟。
5. 在 [應用程式資訊] 頁面上，新增下列資訊：

- **名稱**：輸入要顯示在公司入口網站中的應用程式名稱。

NOTE

如果您在部署及安裝應用程式之後，透過 Intune 變更應用程式名稱，該應用程式將無法再使用命令進行目標。

- **描述**：輸入應用程式的描述。此描述會向公司入口網站中的使用者顯示。
- **Publisher**：輸入此應用程式之發行者的名稱。
- **應用程式 URL**：輸入主控您要指派之應用程式之網站的 url。
- **類別**：(選用)選取一個或多個內建應用程式類別或您建立的類別。這樣做可讓使用者在流覽公司入

口網站時，尋找應用程式的難度。

- **在公司入口網站中將此專案顯示為特色應用程式：**選取此選項，可在使用者流覽應用程式時，在公司入口網站的主要頁面上醒目顯示應用程式套件。
- **需要 managed browser 開啟此連結：**選取此選項可將網站或 web 應用程式的連結指派給使用者，以便在 Intune managed browser 中開啟。此瀏覽器必須安裝在其裝置上。
- **標誌：**Upload 將與應用程式產生關聯的圖示。當使用者流覽公司入口網站時，會隨應用程式一起顯示此圖示。

6. 按 **[下一步]** 顯示 **[範圍標記]** 頁面。

7. 按一下 **[選取範圍 標籤]** 可選擇性地新增應用程式的範圍標記。如需詳細資訊，請參閱 [使用以角色為基礎的存取控制 \(RBAC\) 和範圍標記，以進行發佈](#)。

8. 按 **[下一步]** 顯示 **[工作分派]** 頁面。

9. 選取應用程式的群組指派。如需詳細資訊，請參閱 [新增群組以組織使用者和裝置](#)。

10. 按 **[下一步]** 顯示 **[回顧 + 建立]** 頁面。檢查您為應用程式輸入的值和設定。

11. 完成後，按一下 **[建立]**，將應用程式新增至 Intune。

隨即會顯示您建立之應用程式的 **概述** 刀片。

使用者可以選擇 web 應用程式，然後選擇 **[在瀏覽器中開啟]** 選項，直接從 Windows 公司入口網站應用程式啟動 web 應用程式。發佈的 web URL 會直接在網頁瀏覽器中開啟。

後續步驟

您已建立的應用程式會顯示在 **[應用程式]** 清單中，您可以在其中將其指派給您所選取的群組。如需協助，請參閱 [將應用程式指派給群組](#)。

將內建應用程式新增至 Microsoft Intune

2022/9/27 •

內建應用程式類型可讓您輕鬆地將策劃的受控應用程式，例如Microsoft 365應用程式和協力廠商應用程式指派給 iOS/iPadOS 和 Android 裝置。您可以為此應用程式類型指派特定應用程式，例如Excel、OneDrive、Outlook、Skype等。新增應用程式之後，應用程式類型會顯示為 *內建 iOS 應用程式* 或 *內建 Android 應用程式*。藉由使用內建應用程式類型，您可以選擇要發佈給裝置使用者的應用程式。

在舊版的 Intune 主控台中，Intune提供數個預設的 Managed Microsoft 365 應用程式，例如 Outlook 和 OneDrive。這些受控應用程式的應用程式類型已標記為 *受控 iOS 市集應用程式* 或 *受控 Android 應用程式*。建議您不要使用這些應用程式類型，而是使用內建應用程式類型。藉由使用內建應用程式類型，您可以有額外的彈性來編輯和刪除Microsoft 365應用程式。

NOTE

刪除所有指派時，會從應用程式清單中移除標記為受控 *iOS 市集* 和受控 *Android 應用程式* 的預設Microsoft 365應用程式。

新增內建應用程式

若要在 Microsoft Intune 中將內建應用程式新增至可用的應用程式，請執行下列動作：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 >][所有應用程式 >][新增]。
3. 在 [選取應用程式類型] 窗格的 [可用的其他 類型] 底下，選取 [內建應用程式]。
4. 按一下 [選取]。[新增應用程式] 步驟隨即顯示。
5. 在 [選取內建應用程式] 頁面中，按一下 [選取應用程式] 以選取您要包含的應用程式。
6. 選取您想要包含的內建應用程式。
7. 選取應用程式之後，按一下 [選取內建應用程式] 窗格上的 [選取]。
8. 按一下 [下一步] 以顯示 [範圍標籤] 頁面。
9. 按一下 [選取範圍標籤] 來選擇性地為應用程式新增範圍標籤。如需詳細資訊，請參閱 [針對分散式 IT 使用角色型存取控制 \(RBAC\) 和範圍標籤](#)。
10. 按 [下一步] 以顯示 [指派] 頁面。
11. 選取應用程式的群組指派。如需詳細資訊，請參閱 [新增群組以組織使用者和裝置](#)。
12. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。檢閱您為應用程式輸入的值和設定。
13. 當您完成時，按一下 [建立] 將應用程式新增至Intune。

您所建立應用程式的 [概觀] 刀鋒視窗隨即顯示。

設定應用程式資訊

您可以修改內建應用程式的相關資訊。這項資訊可協助您在Intune中識別應用程式，並協助使用者在公司入口網站中尋找應用程式。

1. 選取 [應用程式 >] [所有應用程式]，然後選取您想要修改的內建應用程式。
內建應用程式的窗格隨即顯示。
2. 選取 [屬性]。
3. 選取 [應用程式資訊] 旁的 [編輯]。
4. 在 [應用程式資訊] 窗格中，您可以修改下列資訊：
 - **名稱**：輸入公司入口網站中顯示的內建應用程式名稱。請確定您使用的所有名稱都是唯一的。如果相同的應用程式名稱存在兩次，公司入口網站中只會向使用者顯示其中一個應用程式。
 - **描述**：輸入應用程式的描述。
 - **Publisher**：輸入應用程式發行者的名稱。
 - **類別**：選擇性地選取一或多個內建應用程式類別。設定此選項可讓使用者在流覽公司入口網站時更容易找到應用程式。
 - **在公司入口網站中將此顯示為精選應用程式**：當使用者流覽應用程式時，在公司入口網站的主頁面上以醒目方式顯示應用程式。
 - **資訊 URL**：選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
 - **隱私權 URL**：選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
 - **開發人員**：選擇性地輸入應用程式開發人員的名稱。
 - **擁有者**：選擇性地輸入此應用程式的擁有者名稱 (例如 *人力資源部門*)。
 - **附注**：輸入您想要與此應用程式相關聯的任何附注。
 - **Upload圖示**：Upload使用者流覽公司入口網站時，隨應用程式一起顯示的圖示。
5. 按一下 [檢閱 + 儲存] 以顯示 [檢閱 + 建立] 頁面。檢閱您為應用程式輸入的值和設定。
6. 當您完成時，按一下 [儲存] 以更新Intune中的應用程式。

您所建立應用程式的 [概觀] 刀鋒視窗隨即顯示。

後續步驟

- 您現在可以將應用程式指派給您選擇的群組。如需詳細資訊，[請參閱將應用程式指派給群組](#)。

將 Android 企業營運應用程式新增至 Microsoft Intune

2022/9/27 •

企業營運 (LOB) 應用程式是您從應用程式安裝檔新增至 Intune 的應用程式。這種類型的應用程式通常是由內部撰寫。Intune 會在使用者的裝置上安裝 LOB 應用程式。

NOTE

如需 LOB 應用程式和 Google Play 開發人員主控台的詳細資訊，請參閱 [受管理的 Google play 私人 \(LOB\) app 使用 Google Developer console 進行發佈](#)。

NOTE

如需 Android Enterprise 裝置，請參閱[使用 Intune 將 Managed Google Play 應用程式新增至 Android Enterprise 裝置](#)。

選取應用程式類型

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 [應用程式] [> > 新增]。
3. 在 [選取應用程式類型] 窗格的 [其他 應用程式類型] 下，選取 [企業營運應用程式]。
4. 按一下 [選取]。隨即會顯示 [新增應用程式] 步驟。

步驟 1-應用程式資訊

選取應用程式套件檔案

1. 在 [新增應用程式] 窗格中，按一下 [選取應用程式套件 檔案]。
2. 在 [應用程式套件 檔案] 窗格中，選取 [流覽] 按鈕。然後，選取副檔名為 apk 的 Android 安裝檔。將會顯示應用程式詳細資料。
3. 當您完成時，請在 [應用程式套件 檔案] 窗格中選取 [確定]，以新增應用程式。

設定應用程式資訊

1. 在 [應用程式資訊] 頁面中，新增應用程式的詳細資料。根據您選取的應用程式，此窗格中的某些值可能會自動填滿。
 - **名稱**：輸入應用程式在公司入口網站中顯示的名稱。請確定您使用的所有應用程式名稱都是唯一的。如果相同的應用程式名稱是兩次，則公司入口網站中只會顯示其中一個應用程式。
 - **描述**：輸入應用程式的描述。描述會顯示在公司入口網站中。
 - **Publisher**：輸入應用程式發行者的名稱。
 - **最低作業系統**：從清單中，選擇可安裝應用程式的最低作業系統版本。如果您將應用程式指派給具有舊版作業系統的裝置，將不會安裝此應用程式。
 - **類別**：選取一個或多個內建應用程式類別，或選取您建立的類別。類別讓使用者在流覽公司入口網站時可輕鬆找到該應用程式。
 - **在公司入口網站中將此專案顯示為特色應用程式**：當使用者流覽應用程式時，會在公司入口網站的主要頁面上醒目顯示應用程式。
 - **資訊 URL**：(選用)輸入包含此應用程式相關資訊的網站 URL。URL 會出現在公司入口網站中。

- **隱私權 URL**：選擇性輸入包含此應用程式隱私權資訊的網站 URL。URL 會出現在公司入口網站中。
- **開發人員**：(選用)輸入應用程式開發人員的名稱。
- **擁有者**：(選擇性)輸入此應用程式擁有者的名稱。例如，HR 部門。
- **附注**：輸入您想要與此應用程式產生關聯的任何附注。
- **標誌**：Upload 與應用程式相關聯的圖示。當使用者流覽公司入口網站時，此圖示會與應用程式一起顯示。

2. 按 [下一步] 顯示 [範圍標記] 頁面。

步驟 2-選取範圍標記 (選用)

您可以使用範圍標記，判斷誰可以查看 Intune 中的用戶端應用程式資訊。如需範圍標籤的完整詳細資料，請參閱 [使用角色型存取控制和範圍標籤來發佈它](#)。

1. 按一下 [選取範圍 標籤] 可選擇性地新增應用程式的範圍標記。
2. 按 [下一步] 顯示 [工作分派] 頁面。

步驟 3-工作分派

1. 為已註冊的裝置 選取 必要 的、可供使用的裝置，或 卸載 應用程式的群組指派。如需詳細資訊，請參閱使用 Microsoft Intune, [新增群組以組織使用者和裝置](#)，並 [指派應用程式至群組](#)。
2. 按 [下一步] 顯示 [回顧 + 建立] 頁面。

步驟 4-審閱 + 建立

1. 檢查您為應用程式輸入的值和設定。
2. 完成後，按一下 [建立]，將應用程式新增至 Intune。

顯示企業營運應用程式的 [概述](#) blade。

步驟5:更新企業營運應用程式

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 [app > 所有應用程式]。
3. 從應用程式清單中尋找並選取您的應用程式。
4. 從應用程式窗格的 [管理] 下，選取 [屬性]。
5. 選取 [App 資訊] 旁的 [編輯]。
6. 在 [選取要更新的檔案] 旁邊，按一下所列出的檔案。隨即會顯示 [應用程式套件 檔案] 窗格。
7. 選取 [資料夾] 圖示，並流覽至更新應用程式檔案的位置。選取 [開啟]。使用套件資訊更新應用程式資訊。
8. 請確認 **應用程式版本** 反映的是更新的應用程式套件。

如果在 Android 裝置上啟用 **來自外部來源的應用程式**，則會在安裝更新之前提示使用者。否則，會自動安裝更新。

NOTE

若要讓 Intune service 成功將新的 APK 檔案部署至裝置，您必須在 `android:versionCode` APK 套件的 AndroidManifest.xml 檔案中增加字串。

後續步驟

- 您建立的應用程式會出現在應用程式清單中。您現在可以將其指派給您所選擇的群組。如需協助，請參

閱 [如何將應用程式指派至群組](#)。

- 深入瞭解您可以監視應用程式之屬性和指派的方式。請參閱 [如何監視應用程式資訊和工作分派](#)。
- 深入瞭解 Intune 中的應用程式內容。請參閱 [裝置和應用程式生命週期的概述](#)。

新增 iOS/iPadOS 的企業營運應用程式 Microsoft Intune

2022/9/27 •

使用本文中的資訊可協助您新增 iOS/iPadOS 的企業營運 (LOB) app Microsoft Intune。企業營運 (LOB) 應用程式是您從 IPA 應用程式安裝檔新增至 Intune 的應用程式。這種類型的應用程式通常是由內部撰寫。您必須先加入 iOS 的開發人員 Enterprise 計畫。如需如何執行此動作的詳細資訊，請參閱 [Apple 的網站](#)。

NOTE

iOS/iPadOS 裝置的使用者可以移除某些內建 iOS/iPadOS 應用程式，例如股票和地圖。您無法使用 Intune 重新部署這些應用程式。若使用者刪除這些應用程式，則必須移至應用程式存放區，並手動重新安裝。

iOS/iPadOS LOB 應用程式的大小上限為每個應用程式 2 GB。

束識別碼 (例如，*com.contoso.app*) 應是應用程式的唯一識別碼。例如，若要在測試目的的實際執行版本旁邊安裝 LOB 應用程式的 Beta 版本，Beta 版本必須具有不同的唯一識別碼 (例如，*com.contoso.app-Beta*)。否則，Beta 版本會與實際執行產生重疊，並被視為升級。重新命名 ipa 檔案不會影響此行為。

您可以將 LOB 應用程式部署到共用 iPad 裝置。針對共用的 iPad 裝置，您必須為包含 Microsoft 端點管理員系統管理中心之共用 iPad 裝置的裝置群組指派 **必要** 的企業營運應用程式。

選取應用程式類型

1. 登入 Microsoft 端點管理員系統 [管理中心](#)。
2. 選取 [應用程式] [> > 新增]。
3. 在 [選取應用程式類型] 窗格的 [其他 應用程式類型] 下，選取 [企業營運應用程式]。
4. 按一下 [選取]。隨即會顯示 [新增應用程式] 步驟。

步驟 1-應用程式資訊

選取應用程式套件檔案

1. 在 [新增應用程式] 窗格中，按一下 [選取應用程式套件 檔案]。
2. 在 [應用程式套件 檔案] 窗格中，選取 [流覽] 按鈕。然後，選取具有 ipa 副檔名的 iOS/iPadOS 安裝檔。將會顯示應用程式詳細資料。
3. 當您完成時，請在 [應用程式套件 檔案] 窗格中選取 [確定]，以新增應用程式。

設定應用程式資訊

1. 在 [應用程式資訊] 頁面中，新增應用程式的詳細資料。根據您選取的應用程式，此窗格中的某些值可能會自動填滿。
 - **名稱**：輸入應用程式在公司入口網站中顯示的名稱。請確定您使用的所有應用程式名稱都是唯一的。如果相同的應用程式名稱是兩次，則公司入口網站中只會顯示其中一個應用程式。
 - **描述**：輸入應用程式的描述。描述會顯示在公司入口網站中。
 - **Publisher**：輸入應用程式發行者的名稱。
 - **最低作業系統**：從清單中，選擇可安裝應用程式的最低作業系統版本。如果您將應用程式指派給具有舊版作業系統的裝置，將不會安裝此應用程式。
 - **類別**：選取一個或多個內建應用程式類別，或選取您建立的類別。類別讓使用者在流覽公司入口網站時可輕鬆找到該應用程式。

- 在公司入口網站中將此專案顯示為特色應用程式：當使用者流覽應用程式時，會在公司入口網站的主要頁面上醒目顯示應用程式。
- 資訊 URL：(選用)輸入包含此應用程式相關資訊的網站 URL。URL 會出現在公司入口網站中。
- 隱私權 URL：選擇性輸入包含此應用程式隱私權資訊的網站 URL。URL 會出現在公司入口網站中。
- 開發人員：(選用)輸入應用程式開發人員的名稱。
- 擁有者：(選擇性)輸入此應用程式擁有者的名稱。例如，HR 部門。
- 附注：輸入您想要與此應用程式產生關聯的任何附注。
- 標誌：Upload 與應用程式相關聯的圖示。當使用者流覽公司入口網站時，此圖示會與應用程式一起顯示。

2. 按 [下一步] 顯示 [範圍標記] 頁面。

步驟 2-選取範圍標記 (選用)

您可以使用範圍標記，判斷誰可以查看 Intune 中的用戶端應用程式資訊。如需範圍標籤的完整詳細資料，請參閱 [使用角色型存取控制和範圍標籤來發佈它](#)。

1. 按一下 [選取範圍 標籤] 可選擇性地新增應用程式的範圍標記。
2. 按 [下一步] 顯示 [工作分派] 頁面。

步驟 3-工作分派

1. 選取所需的註冊裝置、可搭配或不含註冊的功能，或卸載應用程式的群組指派。如需詳細資訊，請參閱使用 Microsoft Intune，[新增群組以組織使用者和裝置，並指派應用程式至群組](#)。
2. 按 [下一步] 顯示 [回顧 + 建立] 頁面。

步驟 4-審閱 + 建立

1. 檢查您為應用程式輸入的值和設定。
2. 完成後，按一下 [建立]，將應用程式新增至 Intune。

顯示企業營運應用程式的概述 blade。

您建立的應用程式現在會顯示在應用程式清單中。您可以從清單中，將應用程式指派給您所選擇的群組。如需協助，請參閱 [如何將應用程式指派至群組](#)。

NOTE

在 iOS/iPadOS LOB app 的布建設定檔中，會有30天的通知，超過此期限便會到期。

步驟5:更新企業營運應用程式

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 [app > 所有應用程式]。
3. 從應用程式清單中尋找並選取您的應用程式。
4. 從應用程式窗格的 [管理] 下，選取 [屬性]。
5. 選取 [App 資訊] 旁的 [編輯]。
6. 在 [選取要更新的檔案] 旁邊，按一下所列出的檔案。隨即會顯示 [應用程式套件 檔案] 窗格。
7. 選取 [資料夾] 圖示，並流覽至更新應用程式檔案的位置。選取 [開啟]。使用套件資訊更新應用程式資訊。
8. 請確認 應用程式版本 反映的是更新的應用程式套件。

系統會自動安裝企業營運應用程式的更新。

NOTE

若要讓 Intune service 成功地将新的 IPA 檔案部署至裝置，您必須更新 IPA 套件中的 plist 檔案中的 CFBundleVersion 字串。您可以透過增加值來升級應用程式，或降低應用程式的降級值，但如果新的應用程式與現有的應用程式相同，則無法上傳新版本的 CFBundleVersion。

後續步驟

- 您建立的應用程式會出現在應用程式清單中。您現在可以將其指派給您所選擇的群組。如需協助，請參閱 [如何將應用程式指派至群組](#)。
- 深入瞭解您可以監視應用程式之屬性和指派的方式。請參閱 [如何監視應用程式資訊和工作分派](#)。
- 深入瞭解 Intune 中的應用程式內容。請參閱 [裝置和應用程式生命週期的概述](#)。

將 Windows 企業營運應用程式新增至 Microsoft Intune

2022/9/27 •

企業營運 (LOB) 應用程式是您從應用程式安裝檔案新增的應用程式。這種應用程式通常是在內部撰寫。下列步驟提供指引，協助您將 Windows LOB 應用程式新增至 Microsoft Intune。

IMPORTANT

使用 .msi 副檔名的安裝檔案部署 Win32 應用程式時，(使用內容準備工具) 封裝在 .intunewin 檔案中，請考慮使用 [Intune 管理延伸模組](#)。如果您在 Autopilot 註冊期間混合安裝 Win32 應用程式和企業營運應用程式，應用程式安裝可能會失敗，因為兩者同時使用信任的安裝程式服務。

選取應用程式類型

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式] > [新增]。
3. 在 [選取應用程式類型] 窗格的 [其他 應用程式類型] 底下，選取 [企業營運應用程式]。
4. 按一下 [選取]。[新增應用程式] 步驟隨即顯示。

步驟 1 - 應用程式資訊

選取應用程式套件檔案

1. 在 [新增應用程式] 窗格中，按一下 [選取應用程式套件檔案]。
2. 在 [應用程式套件檔案] 窗格中，選取瀏覽按鈕。然後，選取副檔名為 .msi、.appx 或 .appxbundle 的 Windows 安裝檔案。將會顯示應用程式詳細資料。

NOTE

Windows 應用程式的副檔名包括 .msi、.appx、.appxbundle、.msix 和 .msixbundle。如需 .msix 的詳細資訊，請參閱 [MSIX 檔](#) 和 [MSIX 應用程式散發](#)。

3. 當您完成時，請在 [應用程式套件檔案] 窗格上選取 [確定] 以新增應用程式。

設定應用程式資訊

1. 在 [應用程式資訊] 頁面中，新增應用程式的詳細資料。視您選擇的應用程式而定，此窗格中的某些值可能會自動填入。
 - **名稱**：輸入出現在公司入口網站中的應用程式名稱。請確定您使用的所有應用程式名稱都是唯一的。如果相同的應用程式名稱存在兩次，公司入口網站中只會出現其中一個應用程式。
 - **描述**：輸入應用程式的描述。描述會出現在公司入口網站中。
 - **發行者**：輸入應用程式的發行者名稱。
 - **應用程式安裝內容**：選取要與此應用程式相關聯的安裝內容。針對雙重模式應用程式，選取此應用程式所需的內容。針對所有其他應用程式，這會根據套件預先選取，而且無法修改。
 - **忽略應用程式版本**：如果應用程式開發人員自動更新應用程式，請設定為 [是]。此選項適用於具有自動更新安裝程式的行動 .msi 應用程式和 Windows 應用程式，(例如 Google Chrome)。
 - **命令列引數**：選擇性地輸入您要在執行時套用至 .msi 檔案的任何命令列引數。範例是 /q。請勿包含

msiexec 命令或引數，例如 /i 或 /x，因為它們會自動使用。如需詳細資訊，請參閱 [命令列選項](#)。如果 MSI 檔案需要額外的命令列選項，請考慮使用 [Win32 應用程式管理](#)。

- **類別**：選取一個或多個內建應用程式類別，或選取您所建立的類別。類別可讓使用者在流覽公司入口網站時更容易找到應用程式。
- **在公司入口網站中將此顯示為精選應用程式**：當使用者流覽應用程式時，在公司入口網站的主頁面上以醒目方式顯示應用程式。
- **資訊 URL**：選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會出現在公司入口網站中。
- **隱私權 URL**：選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會出現在公司入口網站中。
- **開發人員**：選擇性地輸入應用程式開發人員的名稱。
- **擁有者**：選擇性地輸入此應用程式擁有者的名稱。其中一個範例是 **人力資源部門**。
- **附注**：輸入您想要與此應用程式相關聯的任何附注。
- **標誌**：上傳與應用程式相關聯的圖示。當使用者流覽公司入口網站時，此圖示會與應用程式一起顯示。

2. 按一下 [下一步] 以顯示 [範圍標籤] 頁面。

步驟 2 - 選取選用 (範圍標籤)

您可以使用範圍標籤來判斷誰可以在 Intune 中看到用戶端應用程式資訊。如需範圍標籤的完整詳細資料，請參閱 [針對分散式 IT 使用角色型存取控制和範圍標籤](#)。

1. 按一下 [選取範圍標籤] 來選擇性地為應用程式新增範圍標籤。
2. 按 [下一步] 以顯示 [指派] 頁面。

步驟 3 - 指派

1. 選取 [必要]、[適用於已註冊的裝置] 或 [卸載 應用程式的群組指派]。如需詳細資訊，請參閱 [新增群組以組織使用者和裝置](#) 和 [使用 Microsoft Intune 將應用程式指派給群組](#)。
2. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。

步驟 4 - 檢視 + 建立

1. 檢閱您為應用程式輸入的值和設定。
2. 當您完成時，按一下 [建立] 將應用程式新增至 Intune。

隨即顯示企業營運應用程式的 [概觀] 刀鋒視窗。

您建立的應用程式現在會出現在應用程式清單中。從清單中，您可以將應用程式指派給您選擇的群組。如需說明，請參閱 [如何將應用程式指派給群組](#)。

更新企業營運應用程式

1. 登入 Microsoft 端點管理員系統 [管理中心](#)。
2. 選取 [app > 所有應用程式]。
3. 從應用程式清單中尋找並選取您的應用程式。
4. 從應用程式窗格的 [管理] 下，選取 [屬性]。
5. 選取 [App 資訊] 旁的 [編輯]。
6. 在 [選取要更新 的檔案] 旁邊，按一下所列出的檔案。隨即會顯示 [應用程式套件 檔案] 窗格。
7. 選取 [資料夾] 圖示，並流覽至更新應用程式檔案的位置。選取 [開啟]。使用套件資訊更新應用程式資訊。
8. 請確認 **應用程式版本** 反映的是更新的應用程式套件。

NOTE

若要讓Intune服務成功將新的 APPX 檔案部署至裝置，您必須在 APPX 套件的 AppxManifest.xml 檔案中遞增 `Version` 字串。

設定自我更新行動 MSI 應用程式以忽略版本檢查程式

您可以設定已知的自我更新行動 MSI 應用程式來忽略版本檢查程式。

應用程式開發人員或其他更新方法會自動更新某些 MSI 安裝程式型應用程式。針對這些自動更新的 MSI 應用程式，您可以在 [應用程式 資訊] 窗格中設定 [忽略應用程式版本] 設定。當您將此設定切換為 [是] 時，Microsoft Intune不會強制執行安裝在 Windows 用戶端上的應用程式版本。

這項功能有助於避免進入競爭狀況。例如，當應用程式開發人員自動更新應用程式並由Intune更新時，可能會發生競爭狀況。兩者都可能會嘗試在 Windows 用戶端上強制執行應用程式版本，這会造成衝突。

後續步驟

- 您建立的應用程式會出現在應用程式清單中。您現在可以將它指派給您選擇的群組。如需說明，請 [參閱如何將應用程式指派給群組](#)。
- 深入瞭解監視應用程式屬性和指派的方式。請參閱 [如何監視應用程式資訊和指派](#)。
- 深入瞭解應用程式在Intune中的內容。請參閱[Microsoft Intune 中的應用程式生命週期概觀](#)。
- 深入瞭解 Win32 應用程式。請參閱 [Win32 應用程式管理](#)。

簽署企業營運應用程式，使其可以部署到具有 Intune 的 Windows 裝置

2022/9/27 •

身為 Intune 系統管理員，您可以將企業營運 (LOB) 通用應用程式部署到 Windows 8.1 Desktop 或 Windows 10/11 Desktop & Mobile 裝置，包括公司入口網站應用程式。若要將 .appx 應用程式部署至 Windows 8.1 Desktop 或 Windows 10/11 Desktop & Mobile 裝置，您可以使用來自 Windows 裝置已信任之公開憑證授權單位單位的程式碼簽署憑證，也可以使用您自己的憑證授權單位單位。

NOTE

Microsoft Intune 將於 2022 年 10 月 21 日終止對執行 Windows 8.1 之裝置的支援。Intune 將不再支援側載 Windows 8.1。

Windows 8.1 電腦需要企業原則啟用側載或使用側載金鑰，(針對已加入網域的裝置自動啟用)。如需詳細資訊，請參閱 [Windows 8 側載](#)。

Windows 10/11 側載

在 Windows 10/11 中，側載與舊版 Windows 不同：

- 您可以使用企業原則解除鎖定裝置以進行側載。Intune 提供稱為「受信任的應用程式安裝」的裝置設定原則。若裝置已信任用來簽署 appx 應用程式的憑證，則需要將此設定設為 **允許**。
- 不需要 Symantec 電話憑證和側載授權金鑰。不過，如果內部部署憑證授權單位單位無法使用，您可能需要從公開憑證授權單位單位取得程式碼簽署憑證。如需詳細資訊，請參閱 [程式碼簽署簡介](#)。

程式碼簽署您的應用程式

第一個步驟是撰寫 appx 套件的程式碼。如需詳細資訊，請參閱 [使用 SignTool 簽署應用程式套件](#)。

上傳您的應用程式

接下來，您必須上傳已簽署的 appx 檔案。如需詳細資訊，請參閱 [將 Windows 企業營運應用程式新增至 Microsoft Intune](#)。

如果您視需要將應用程式部署給使用者或裝置，則不需要 Intune 公司入口網站應用程式。不過，如果您將應用程式部署為可供使用者使用，則他們可以從公用 Microsoft Store 使用公司入口網站應用程式、從私人商務用 Microsoft Store 使用公司入口網站應用程式，或者您必須簽署並手動部署 Intune 公司入口網站應用程式。

上傳程式碼簽署憑證

如果您的 Windows 10/11 裝置尚未信任憑證授權單位單位，則在您簽署 appx 套件並將其上傳至 Intune 服務之後，您必須使用下列步驟將程式碼簽署憑證上傳至 Intune：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 按一下 [租使用者系統管理 > 連接器和權杖 >] [Windows 企業憑證]。
3. 選取 [程式碼簽署憑證檔案] 底下的檔案。
4. 選取您的 .cer 檔案，然後按一下 [開啟]。
5. 按一下 [上傳] 將憑證檔案新增至 Intune。

現在，任何 Windows 10/11 Desktop & 行動裝置搭配 Intune 服務的 appx 部署，都會自動下載對應的企業憑證，且應用程式將可在安裝後啟動。

Intune 只會部署已上傳的最新 .cer 檔案。如果您有多個由不同開發人員所建立的 appx 檔案，而這些檔案與您的

組織沒有關聯，則您必須讓他們提供未簽署的 appx 檔案以使用您的憑證進行簽署，或提供貴組織所使用的程式碼簽署憑證。

如何更新 Symantec 企業程式碼簽署憑證

用來部署 Windows Phone 8.1 行動裝置應用程式的憑證已于 2019 年 2 月 28 日中止，無法再從 Symantec 更新。此外，自 2020 年 8 月 10 日起，Intune 已終止 Windows 10 行動裝置的支援。

如何為企業營運 (LOB) 應用程式安裝更新的憑證

Windows Phone 8.1

一旦現有的 Symantec Mobile Enterprise 程式碼簽署憑證過期，Intune 服務就無法再為此平臺部署 LOB 應用程式。

Windows 8.1 Desktop/Windows 10 Desktop & Mobile

如果憑證期間已過期，appx 檔案可能會停止啟動。您應該取得新的 .cer 檔案，並遵循指示以程式碼簽署每個已部署的 appx 檔案，並將所有 appx 檔案和更新的 .cer 檔案重新上傳至 Microsoft 端點管理員系統管理中心內 Intune 的 [Windows 企業憑證] 區段。

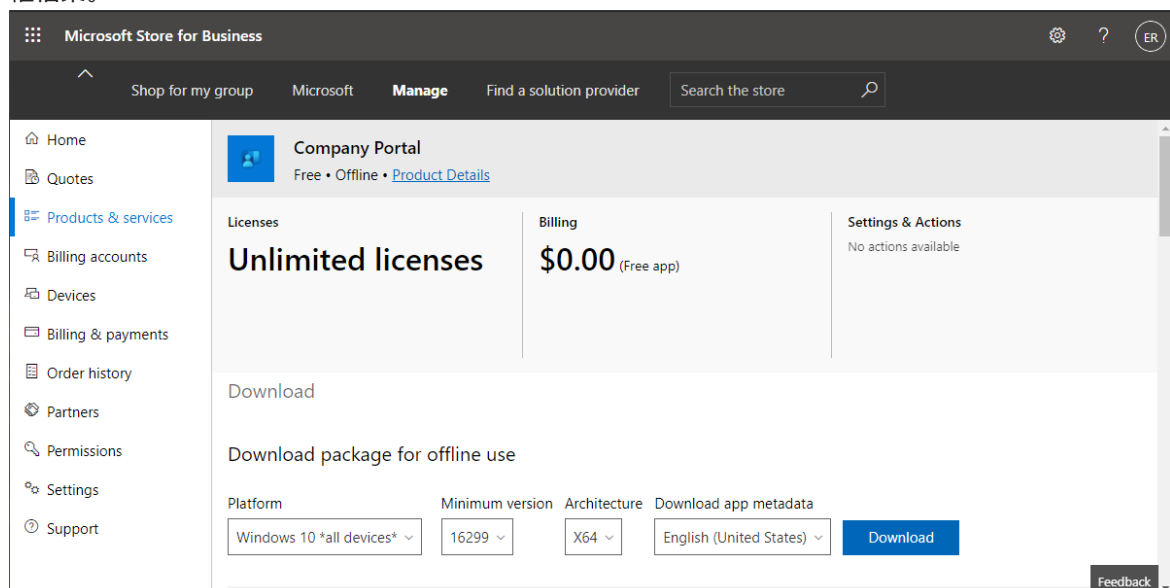
手動部署 Windows 10 公司入口網站應用程式

如果您不想提供 Microsoft Store 的存取權，即使您尚未將 Intune 與商務用 Microsoft Store (MSFB) 整合，也可以直接從 Intune 手動部署 Windows 10 公司入口網站應用程式。或者，如果您已整合，則可以[使用 MSFB 部署應用程式來部署](#)公司入口網站應用程式。

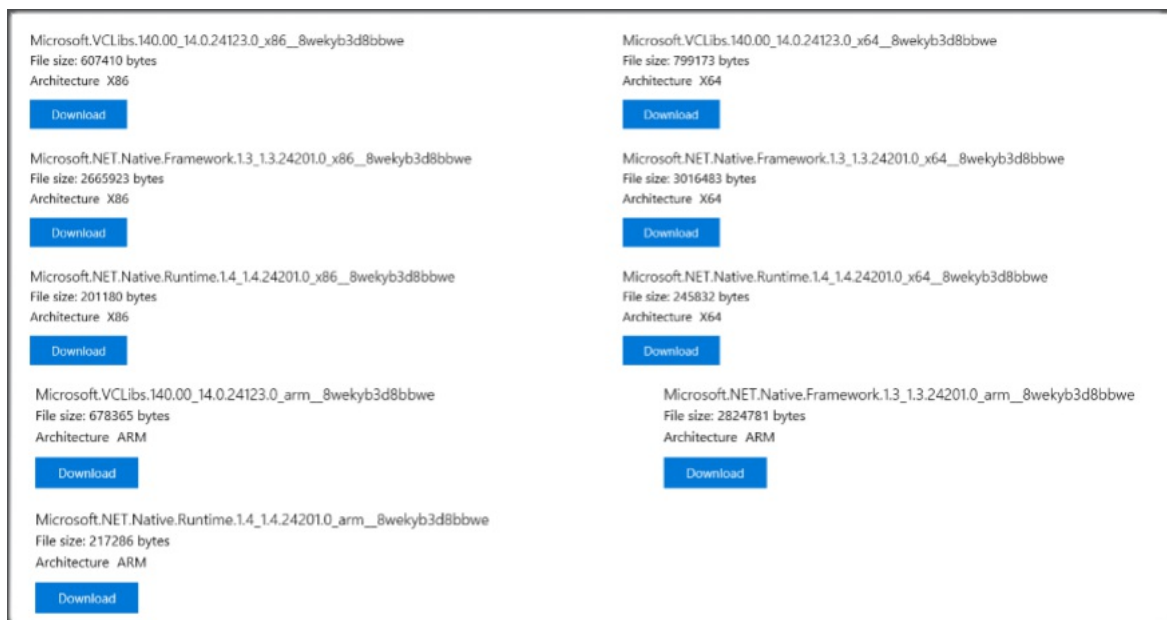
NOTE

每次發行應用程式更新時，此選項都需要部署手動更新。

1. 在 [商務用 Microsoft Store](#) 中登入您的帳戶，並取得公司入口網站應用程式的 **離線授權** 版本。
2. 取得應用程式之後，請在 [清查] 頁面中選取應用程式。
3. 選 **Windows 10 所有裝置** 作為 [平臺]，然後選取適當的 [架構] 並下載。此應用程式不需要應用程式授權檔案。

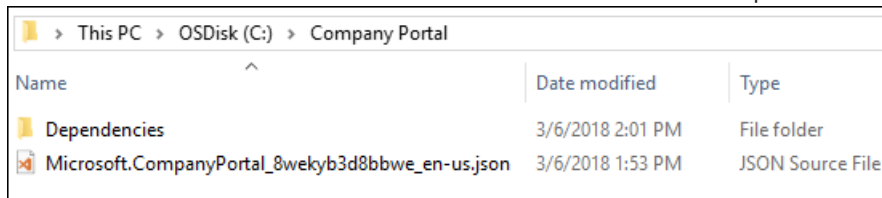


4. 下載「必要架構」下的所有套件。這必須針對 x86、x64、ARM 和 ARM64 架構來完成，因此總共有 9 個套件，如下所示。



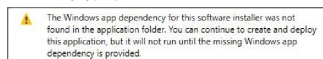
5. 將公司入口網站應用程式上傳至 Intune 之前，請先建立資料夾 (例如 C:\公司入口網站)，並以下列方式建構套件：

a. 將公司入口網站套件放入 C:\公司入口網站。也請在此位置建立 Dependencies 子資料夾。



b. 將九個相依性套件放在 [相依性] 資料夾中。

如果相依性不是以這種格式放置，Intune 將無法在套件上傳期間辨識和上傳它們，導致上傳失敗併發生下列錯誤。



6. 返回 Intune，然後將公司入口網站應用程式上傳為新的應用程式。將它部署為所需目標使用者集合的必要應用程式。

如需 Intune 如何處理通用應用程式相依性的詳細資訊，請參閱 [透過 Microsoft Intune MDM 部署具有相依性的 appxbundle](#)。

如果使用者已從市集安裝較舊的應用程式，如何?更新使用者裝置上的公司入口網站？

如果您的使用者已從市集安裝 Windows 8.1 公司入口網站應用程式，則應該會自動更新為新版本，而不需要您或您的使用者採取任何動作。如果未進行更新，請要求您的使用者檢查他們是否已在其裝置上啟用市集應用程式的自動更新。

如何?將我的側載 Windows 8.1 公司入口網站應用程式升級至 Windows 10 公司入口網站應用程式？

我們建議的移轉路徑是藉由將部署動作設定為 [卸載] 來刪除 Windows 8.1 公司入口網站應用程式的部署。完成此動作之後，即可使用上述任何選項來部署 Windows 10 公司入口網站應用程式。

如果您需要側載應用程式並部署 Windows 8.1 公司入口網站，而不需使用 Symantec 憑證簽署它，請遵循上述直接透過 Intune 部署一節中的步驟來完成升級。

如果您需要側載應用程式，而且您已使用 Symantec 程式碼簽署憑證簽署並部署 Windows 8.1 公司入口網站，請遵循下一節中的步驟。

如何?將已簽署並側載的 Windows 8.1 公司入口網站應用程式升級至 Windows 10 公司入口網站應用程式？

我們建議的移轉路徑是藉由將部署動作設定為 [卸載] 來刪除 Windows 8.1 公司入口網站應用程式的現有部署。完成此動作之後，即可正常部署 Windows 10 公司入口網站應用程式。

否則，必須適當地更新和簽署Windows 10 公司入口網站應用程式，以確保遵守升級路徑。

如果以這種方式簽署並部署Windows 10 公司入口網站應用程式，則您必須在市場集中提供每個新應用程式更新時重複此程式。更新市場時，應用程式不會自動更新。

以下是以這種方式簽署和部署應用程式的方式：

1. 下載[Windows 10 公司入口網站](#)的[Microsoft Intune簽署腳本](#)。此腳本需要將 Windows SDK for Windows 10 安裝在主機電腦上。若要下載 Windows SDK，請參閱 [Windows 10 SDK for Windows 10](#)。
2. 從商務用 Microsoft Store下載Windows 10 公司入口網站應用程式，如上所述。
3. 使用腳本標頭中詳述的輸入參數執行腳本，以簽署Windows 10 公司入口網站應用程式，(解壓縮如下)。相依性不需要傳遞至腳本。只有當應用程式上傳至 Intune 管理員 主控台時，才需要這些專案。

“	“
InputWin10AppxBundle	來源 appxbundle 檔案所在的路徑。
OutputWin10AppxBundle	已簽署 appxbundle 檔案的輸出路徑。
Win81Appx	Windows 8.1 公司入口網站 (的路徑。APPX) 檔案。
PfxFilePath	Symantec Enterprise Mobile Code 簽署憑證的路徑 (。PFX) 檔案。
PfxPassword	Symantec Enterprise Mobile Code 簽署憑證的密碼。
PublisherId	企業的發行者識別碼。如果不存在，則會使用 Symantec Enterprise Mobile Code 簽署憑證的 [主旨] 欄位。
SdkPath	適用於 Windows 10 之 Windows SDK 根資料夾的路徑。此引數是選擇性的，預設為 <code>\$(env:ProgramFiles (x86))\Windows Kits\10</code>

腳本會在Windows 10 公司入口網站應用程式完成執行時輸出已簽署的版本。然後，您可以透過 Intune 將已簽署的應用程式版本部署為 LOB 應用程式，這會將目前部署的版本升級至這個新的應用程式。

如何將 macOS 企業營運 (LOB) 應用程式新增至 Microsoft Intune

2022/9/27 •

使用本文中的資訊，協助您將 macOS 企業營運應用程式新增至 Microsoft Intune。

NOTE

從 macOS Catalina 10.15 的發行開始，在將您的應用程式新增至 Intune 之前，請先檢查以確定您的 macOS LOB 應用程式已標示。如果您 LOB 應用程式的開發人員未將其應用程式標示，應用程式將無法在使用者的 macOS 裝置上執行。如需如何檢查應用程式是否已標示的詳細資訊，請造訪 [將 macOS 應用程式命名為 Notarize 以準備 macOS Catalina](#)。

macOS LOB 應用程式的大小上限為每個應用程式 2 GB。

雖然 macOS 裝置的使用者可以移除某些內建的 macOS 應用程式，例如股票和地圖，但您無法使用 Intune 來重新部署這些應用程式。如果終端使用者刪除這些應用程式，他們必須移至應用程式市集，並手動重新安裝它們。

選取應用程式類型

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式] > [新增]。
3. 在 [選取應用程式類型] 窗格的 [其他 應用程式類型] 底下，選取 [企業營運應用程式]。
4. 按一下 [選取]。[新增應用程式] 步驟隨即顯示。

步驟 1 - 應用程式資訊

NOTE

上傳 .pkg 檔案  是 macOS 10.14。

選取應用程式套件檔案

1. 在 [新增應用程式] 窗格中，按一下 [選取應用程式套件檔案]。
2. 在 [應用程式套件檔案] 窗格中，選取瀏覽按鈕。然後，選取副檔名為 .pkg 的 macOS 安裝檔案。將會顯示應用程式詳細資料。
3. 當您完成時，請在 [應用程式套件檔案] 窗格上選取 [確定] 以新增應用程式。

設定應用程式資訊

1. 在 [應用程式資訊] 頁面中，新增應用程式的詳細資料。視您選擇的應用程式而定，此窗格中的某些值可能會自動填入。
 - **名稱**：輸入出現在公司入口網站中的應用程式名稱。請確定您使用的所有應用程式名稱都是唯一的。如果相同的應用程式名稱存在兩次，公司入口網站中只會出現其中一個應用程式。
 - **描述**：輸入應用程式的描述。描述會出現在公司入口網站中。
 - **發行者**：輸入應用程式的發行者名稱。
 - **最小作業系統**：從清單中，選擇可安裝應用程式的最低作業系統版本。如果您將應用程式指派給具有舊版作業系統的裝置，則不會安裝該應用程式。
 - **忽略應用程式版本**：如果應用程式尚未安裝在裝置上，請選取 [是] 以安裝應用程式。選取 [否]，只在尚未安裝在裝置上，或部署應用程式的版本號碼不符合裝置上已安裝的版本時，才安裝應用程式。

- **安裝為受控**：選取 [是] 以在支援的裝置上將 Mac LOB 應用程式安裝為受控應用程式，(macOS 11 和更新版本)。macOS LOB 應用程式只能在應用程式可散發包含不含任何巢狀套件的單一應用程式並安裝至 `/Applications` 目錄時，以受控方式安裝。受管理的企業營運應用程式將能夠在支援的裝置上使用卸載 指派類型來移除，(macOS 11 和更新版本)。此外，移除 MDM 設定檔會從裝置移除所有受控應用程式。預設值為 [否]。
- **包含的應用程式**：檢閱和編輯上傳檔案中包含的應用程式。包含的應用程式套件組合識別碼和組建編號可用來偵測和監視已上傳檔案的應用程式安裝狀態。第一個列出的應用程式會當做應用程式報告中的主要應用程式使用。
包含的應用程式清單應該只包含已上傳檔案在 Mac 上 [應用程式] 資料夾中 所安裝的應用程式 ()。您應該從 [包含的 應用程式] 清單中移除不是應用程式或未安裝到 [應用程式] 資料夾的任何其他檔案類型。如果 包含的應用程式 清單包含非應用程式的檔案，或未安裝所有列出的應用程式，則應用程式安裝狀態不會回報成功。
Mac 終端機可用來查閱並確認已安裝應用程式的內含應用程式詳細資料。
例如，若要查閱套件組合識別碼和公司入口網站組建編號，請執行下列命令：
預設值為 `/Applications/Company\ Portal.app/Contents/Info CFBundleIdentifier`
然後，執行下列命令：
預設值為 `/Applications/Company\ Portal.app/Contents/Info CFBundleShortVersionString`
- **類別**：選取一或多個內建應用程式類別，或選取您所建立的類別。類別可讓使用者在流覽公司入口網站時更容易找到應用程式。
- **在公司入口網站中將此顯示為精選應用程式**：當使用者流覽應用程式時，在公司入口網站的主頁面上以醒目方式顯示應用程式。
- **資訊 URL**：選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會出現在公司入口網站中。
- **隱私權 URL**：選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會出現在公司入口網站中。
- **開發人員**：選擇性地輸入應用程式開發人員的名稱。
- **擁有者**：選擇性地輸入此應用程式擁有者的名稱。其中一個範例是 人力資源部門。
- **附注**：輸入您想要與此應用程式相關聯的任何附注。
- **標誌**：上傳與應用程式相關聯的圖示。當使用者流覽公司入口網站時，此圖示會與應用程式一起顯示。

2. 按一下 [下一步] 以顯示 [範圍標籤] 頁面。

步驟 2 - 選取選用 (範圍標籤)

您可以使用範圍標籤來判斷誰可以在Intune中看到用戶端應用程式資訊。如需範圍標籤的完整詳細資料，請 [參閱針對分散式 IT 使用角色型存取控制和範圍標籤](#)。

1. 按一下 [選取範圍標籤] 來選擇性地為應用程式新增範圍標籤。
2. 按 [下一步] 以顯示 [指派] 頁面。

步驟 3 - 指派

1. 選取 [必要]、[適用於已註冊的裝置] 或 [卸載 應用程式的群組指派]。如需詳細資訊，請 [參閱新增群組以組織使用者和裝置和使用Microsoft Intune將應用程式指派給群組](#)。

NOTE

只有在 [安裝 ■ Managed] 設定為 [是] 的情況下建立的 LOB 應用程式，才會顯示 [卸載意圖]。如需詳細資訊，請檢閱本文稍早的 **■**。

2. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。

步驟 4 - 檢閱 + 建立

1. 檢閱您為應用程式輸入的值和設定。
2. 當您完成時，按一下 [建立] 將應用程式新增至Intune。

隨即顯示企業營運應用程式的 [概觀] 刀鋒視窗。

您建立的應用程式會出現在應用程式清單中，您可以將它指派給您選擇的群組。如需說明，請 [參閱如何將應用程式指派給群組](#)。

NOTE

如果 *.pkg* 檔案包含多個應用程式或應用程式安裝程式，則Microsoft Intune只會報告在裝置上偵測到所有已安裝的應用程式時，*應用程式* 已成功安裝。

更新企業營運應用程式

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 [app > 所有應用程式]。
3. 從應用程式清單中尋找並選取您的應用程式。
4. 從應用程式窗格的 [管理] 下，選取 [屬性]。
5. 選取 [App 資訊] 旁的 [編輯]。
6. 在 [選取要更新 的檔案] 旁邊，按一下所列出的檔案。隨即會顯示 [應用程式套件 檔案] 窗格。
7. 選取 [資料夾] 圖示，並流覽至更新應用程式檔案的位置。選取 [開啟]。使用套件資訊更新應用程式資訊。
8. 請確認 **應用程式版本** 反映的是更新的應用程式套件。

若要更新部署為 *.pkg* 檔案的企業營運應用程式，您必須遞增 `CFBundleShortVersionString` *.pkg* 檔案的。

Intune會在經過此排程時更新應用程式，前提是裝置上仍存在任何舊版的應用程式。

後續步驟

- 您建立的應用程式會顯示在應用程式清單中。您現在可以將它指派給您選擇的群組。如需說明，請 [參閱如何將應用程式指派給群組](#)。
- 深入瞭解監視應用程式屬性和指派的方式。如需詳細資訊，請 [參閱如何監視應用程式資訊和指派](#)。
- 深入瞭解應用程式在Intune中的內容。如需詳細資訊，請參閱 [裝置和應用程式生命週期概觀](#)

Microsoft Intune macOS 的管理代理程式

2022/9/27 •

為什麼需要代理程式？

Microsoft Intune 管理代理程式必須安裝在受管理的 macOS 裝置上，才能啟用原生 macOS 作業系統不支援的高級裝置管理功能。

代理程式如何安裝？

在 Intune 管理的 macOS 裝置上，系統會自動並以無訊息方式安裝代理程式，您必須在 Microsoft 端點管理員系統管理中心指派至少一個命令介面腳本。代理程式會在適用的位置 `/Library/Intune/Microsoft Intune Agent.app` 安裝，而且不會出現在 macOS 裝置上的 **Finder > 應用程式** 中。在 macOS 裝置上執行 agent 時，代理程式就會顯示在 [`IntuneMdmAgent` 活動監視器] 中。

代理程式的功能為何？

- 代理程式會在簽入以接收 macOS 裝置的指派命令介面腳本之前，以無訊息的方式驗證 Intune 服務。
- 代理程式會收到指派的命令介面腳本，並根據系統管理員所設定的排程、重試嘗試、通知設定及其他設定來執行腳本。
- 代理程式通常會以 Intune 服務檢查新的或更新的腳本，但通常每8小時檢查一次。此簽入程式獨立于 MDM 簽入過程。

如何從 Mac 手動啟動代理程式簽入？

在已安裝代理的受管理 Mac 上，開啟 **公司入口網站**，選取本機裝置，然後按一下 [檢查設定]。這會啟動 MDM 簽入和代理程式簽入。

或者，開啟 [終端]，執行 `sudo killall IntuneMdmAgent` 命令終止 `IntuneMdmAgent` 處理常式。`IntuneMdmAgent` 程式將立即重新開機，該程式會使用 Intune 初始化存回。

NOTE

Microsoft 端點管理員系統管理主控台中裝置的 Sync 動作會啟動 MDM 簽入，而不會強制執行代理程式簽入。

何時移除代理程式？

有幾種情況可能會導致代理程式從裝置中移除，例如：

- 命令介面腳本不再指派給裝置。
- 已不再管理 macOS 裝置。
- 代理程式在24小時內處於不可恢復的狀態 (裝置-清醒時間)。

為何即使不再管理 Mac 也會執行腳本？

當您已不再管理具有指派腳本的 Mac 時，不會立即移除代理程式。代理程式會在下一個代理程式檢查時，偵測不會管理該 Mac (每8小時) 並取消排程腳本執行。因此，排定執行的任何本機儲存的腳本，要比下一個排程的代理程式簽入執行的頻率要高。當代理程式無法存回時，它會在最多24小時內重新嘗試存回 (裝置-清醒時間) 然後從 Mac 自行移除。

如何關閉傳送給 Microsoft 以進行命令介面腳本的使用狀況資料？

若要關閉從 Intune 管理代理程式傳送給 Microsoft 的使用狀況資料，請開啟公司入口網站並選取 **功能表 > 偏好 > 複選 '允許 Microsoft 收集流量資料'**。這樣會關閉同時傳送給代理程式和公司入口網站的使用方式資料。

後續步驟

- 您建立的應用程式會顯示在 [應用程式] 清單中。您現在可以將其指派給您所選擇的群組。如需協助，請參閱 [如何將應用程式指派至群組](#)。
- 深入瞭解您可以監視應用程式之屬性和指派的方式。如需詳細資訊，請參閱 [如何監視應用程式資訊和工作分派](#)。
- 深入瞭解 Intune 中的應用程式內容。如需詳細資訊，請參閱 [裝置和應用程式生命週期一覽](#)

將 macOS DMG 應用程式新增至 Microsoft Intune

2022/9/27 •

NOTE

此功能處於公開預覽狀態。

使用本文中的資訊，協助您將 macOS DMG 應用程式新增至 Microsoft Intune。DMG 應用程式是包含其中一或多個應用程式的磁片映射檔。許多適用於 macOS 的常見應用程式都可使用 DMG 格式。如需如何建立磁片映射檔案的詳細資訊，請參閱 [Apple 的網站](#)。

NOTE

DMG 檔案必須包含一或多個副檔名為 .app 的檔案。將不會安裝包含其他安裝程式檔案類型的 DMG 檔案。

必要條件

在 macOS 裝置上安裝 macOS DMG 應用程式之前，必須符合下列必要條件。

- 裝置是由 Intune 管理。
- DMG 應用程式的大小小於 2GB。
- 已安裝 [適用於 macOS 的 Microsoft Intune 管理代理程式](#)。

部署 DMG 應用程式的重要考慮

單一 DMG 應該只包含單一應用程式檔或相依于彼此的多個應用程式檔。包含的應用程式檔案可以列在 [偵測規則] 索引標籤的 [包含的應用程式] 區段下方，以便從要在報表中使用的父應用程式開始。

不建議使用相同的 DMG 檔案來安裝不相依于彼此的多個應用程式。如果使用相同的 DMG 應用程式部署多個獨立應用程式，若無法安裝一個應用程式，將會重新安裝其他應用程式。在此情況下，監視報告也會將 DMG 安裝視為失敗。

選取應用程式類型

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式] > [新增]。
3. 在 [選取應用程式類型] 窗格的 [其他 應用程式類型] 底下，選取 [macOS 應用程式 (DMG)]。
4. 按一下 [選取]。[新增應用程式] 步驟隨即顯示。

步驟 1 – 應用程式資訊

選取應用程式套件檔案：

1. 在 [新增應用程式] 窗格中，按一下 [選取應用程式套件檔案]。
2. 在 [應用程式套件檔案] 窗格中，選取瀏覽按鈕。然後，選取副檔名為 .dmg 的 macOS DMG 檔案。將會顯示應用程式詳細資料。
3. 當您完成時，請在 [應用程式套件檔案] 窗格上選取 [確定] 以新增應用程式。

設定應用程式資訊

1. 在 [應用程式資訊] 頁面中，新增應用程式的詳細資料。視您選擇的應用程式而定，此窗格中的某些值可能會自動填入。

- **名稱**：輸入出現在原則名稱和公司入口網站中的應用程式名稱。請確定您使用的所有應用程式名稱都是唯一的。如果相同的應用程式名稱存在兩次，公司入口網站中只會出現其中一個應用程式。
- **描述**：輸入應用程式的描述。描述會出現在公司入口網站中。
- **發行者**：輸入應用程式的發行者名稱。
- **類別**：選取一個或多個內建應用程式類別，或選取您所建立的類別。類別可讓使用者在流覽公司入口網站時更容易找到應用程式。
- **資訊 URL**：選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會出現在公司入口網站中。
- **隱私權 URL**：選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會出現在公司入口網站中。
- **開發人員**：選擇性地輸入應用程式開發人員的名稱。
- **擁有者**：選擇性地輸入此應用程式擁有者的名稱。其中一個範例是人力資源部門。
- **附注**：輸入您想要與此應用程式相關聯的任何附注。
- **標誌**：上傳與應用程式相關聯的圖示。當使用者流覽公司入口網站時，此圖示會與應用程式一起顯示。

2. 按 [下一步] 以設定需求。

步驟 2 – 需求

您可以選擇安裝此應用程式所需的最低作業系統。

最小作業系統：從清單中，選擇可安裝應用程式的最低作業系統版本。如果您將應用程式指派給具有舊版作業系統的裝置，則不會安裝該應用程式。

步驟 3 – 偵測規則

您可以使用偵測規則來選擇在受控 macOS 裝置上偵測到應用程式安裝的方式。

忽略應用程式版本：如果應用程式尚未安裝在裝置上，請選取 [是] 以安裝應用程式。這只會尋找應用程式套件組合識別碼的存在。針對具有自動更新機制的應用程式，選取 [是]。如果應用程式尚未安裝在裝置上，或部署應用程式的版本號碼不符合裝置上已安裝的版本，請選取 [否] 來安裝應用程式。

NOTE

若 ■ 群組指派，請考慮 [■] 設定。當 [■] 設定為 [■] 時，應用程式套件組合識別碼和版本號碼必須相符，才能移除應用程式。當 [■] 設定為 [■] 時，只有應用程式套件組合識別碼必須相符才能移除應用程式。

包含的應用程式：提供包含在已上傳檔案中的應用程式。包含的應用程式套件組合識別碼和組建編號可用來偵測和監視已上傳檔案的應用程式安裝狀態。包含的應用程式清單應該只包含已上傳檔案在 Mac 上 [應用程式] 資料夾中所安裝的應用程式 ()。任何其他類型的檔案，不是應用程式或未安裝至應用程式資料夾的應用程式，都應該從 [包含的應用程式] 清單中排除。如果包含的應用程式清單包含非應用程式的檔案，或未安裝所有列出的應用程式，則應用程式安裝狀態不會回報成功。

NOTE

- 當 DMG 檔案中有多個應用程式時，會使用 [包含的應用程式] 清單上的第一個應用程式來識別應用程式。
- Mac 終端機可用來查閱並確認已安裝應用程式的內含應用程式詳細資料。例如，若要查閱套件組合識別碼和公司入口網站組建編號，請執行下列命令：

```
defaults read /Applications/Company\ Portal.app/Contents/Info CFBundleIdentifier
```

然後，執行下列命令：

```
defaults read /Applications/Company\ Portal.app/Contents/Info CFBundleShortVersionString
```

- 或者，`CFBundleIdentifier` 和 `CFBundleShortVersionString` 可以在 Mac 上掛接的 DMG 檔案檔案底下 `<app_name>.app/Contents/Info.plist` 找到。

步驟 4 – 選取選用 () 範圍標籤

您可以使用範圍標籤來判斷誰可以在Intune中看到用戶端應用程式資訊。如需範圍標籤的完整詳細資料，請 [參閱針對分散式 IT 使用角色型存取控制和範圍標籤](#)。1. 按一下 [選取範圍標籤] 來選擇性地為應用程式新增範圍標籤。2. 按 [下一步] 以顯示 [指派] 頁面。

步驟 5 - 指派

您可以選取應用程式的 [必要] 或 [卸載] 群組指派。如需詳細資訊，請 [參閱新增群組以組織使用者和裝置和使用Microsoft Intune將應用程式指派給群組](#)。

NOTE

當裝置淘汰時，使用 Intune 代理程式部署的 macOS 應用程式將不會自動從裝置中移除。其包含的應用程式和資料會保留在裝置上。建議您在淘汰裝置之前先移除應用程式。

1. 針對特定應用程式，選取指派類型：

- 必要**：應用程式會安裝到 `/Applications/` 所選群組中裝置上的目錄。
- 卸載**：應用程式會從 `/Applications/` 所選群組中裝置上的目錄卸載。

2. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。

步驟 6 – 檢視 + 建立

- 檢視您為應用程式輸入的值和設定。
- 當您完成時，按一下 [建立] 將應用程式新增至Intune。隨即顯示 macOS DMG 應用程式的 [概觀] 窗格。

您建立的應用程式會出現在應用程式清單中，您可以將它指派給您選擇的群組。如需說明，請 [參閱如何將應用程式指派給群組](#)。

NOTE

如果 `.dmg` 檔案包含多個應用程式，則Microsoft Intune只會報告在裝置上偵測到所有已安裝的應用程式時，應用程式已成功安裝。

後續步驟

- 您建立的應用程式會顯示在應用程式清單中。您現在可以將它指派給您選擇的群組。如需說明，請 [參閱如何](#)

將應用程式指派給群組。

- 深入瞭解監視應用程式屬性和指派的方式。如需詳細資訊，請參閱[如何監視應用程式資訊和指派](#)。
- 深入瞭解應用程式在Intune中的內容。如需詳細資訊，請參閱[裝置和應用程式生命週期概觀](#)

已知問題

- 「適用於已註冊的裝置」指派類型無法使用：目前僅支援 **必要** 和 **卸載** 指派類型。
- 「收集記錄」動作在預覽期間無法使用：macOS 應用程式上的記錄收集功能 (DMG) 在預覽期間無法使用。
- 在預覽期間，錯誤可能不會顯示詳細資料：您遇到的某些錯誤可能只會顯示錯誤碼的「失敗」狀態，而不會提供其他詳細資料。
- 應用程式升級無法安裝：無法安裝與應用程式資料夾中現有應用程式具有相同套件組合識別碼或相同名稱的應用程式。
- DMG 應用程式會在部署後回報一次：指派的 DMG 應用程式只會在初始部署時回報。這些應用程式不會在預覽期間再次回報。
- 某些 DMG 應用程式可能會在啟動時對終端使用者顯示警告：從網際網路下載並使用 Intune 部署的應用程式可能會在啟動時對終端使用者顯示警告。終端使用者可以在對話方塊上按一下 [開啟]，以繼續開啟應用程式。



- 某些應用程式圖示在安裝後可能不會立即顯示：某些應用程式圖示在安裝之後可能需要一些時間，才能開始顯示在已安裝的裝置上。
- 監視報告只會顯示錯誤碼：失敗的應用程式安裝只會在「裝置狀態」監視報告中顯示錯誤碼。若要顯示錯誤詳細資料，請重新整理瀏覽器視窗，或參閱疑難排解一節中的資料表。

疑難排解

macOS 應用程式安裝可能因為下表中提供的下列任何原因而無法成功。若要解決這些錯誤，請遵循補救步驟。如果應用程式仍被指派，則會在下一次代理程式簽入時重試失敗的安裝。

錯誤碼	原因	補救措施
0x87D30137	裝置不符合系統管理員設定的最低 OS 需求。	將 macOS 更新為系統管理員所需的最低 OS 版本。
0x87D3013E	DMG 檔案不包含任何支援的應用程式。它必須至少包含一個 .app 檔案。	請確定上傳的檔案包含一或多個 .app 檔案。
0x87D30139	無法掛接 DMG 檔案以進行安裝。如果錯誤持續發生，請檢查 DMG 檔案。	請嘗試手動掛接 DMG 檔案，以確認磁片區載入成功。

III	IIII	IIII
0x87D3013B	應用程式無法安裝到應用程式目錄。同步裝置以重試安裝應用程式。	確定裝置可以在本機將應用程式安裝到應用程式目錄。
0x87D3012F、0x87D30130、0x87D30133、0x87D30134、0x87D30136、	無法安裝應用程式, 因為發生內部錯誤。如果錯誤持續發生, 請連絡Intune支援。	使用 Intune 安裝應用程式時發生錯誤。請嘗試手動安裝應用程式, 或嘗試建立包含應用程式的新 macOS 應用程式佈建檔。如果錯誤持續發生, 請連絡 Intune支援。
0x87D30131、0x87D30132	無法下載應用程式。同步裝置以重試安裝應用程式。	下載應用程式時發生錯誤。如果網路不佳或應用程式大小很大, 就可能發生這種情況。
0x87D30135	無法安裝應用程式, 因為發生裝置錯誤。同步裝置以重試安裝應用程式。	這可能是因為磁碟空間不足, 或應用程式無法寫入資料夾。確定裝置可以將應用程式安裝到 [應用程式] 資料夾。
0x87D3013A	此磁片的實體資源已用盡。	這可能是因為硬碟空間不足或安裝檔案的二進位檔損毀所造成。修正硬碟空間, 然後重新開機Microsoft Intune管理延伸模組服務, 然後再試一次。

Microsoft Intune中的 Win32 應用程式管理

2022/9/27 •

Microsoft Intune允許 Win32 應用程式管理功能。雖然雲端連線客戶可以使用 Microsoft 端點Configuration Manager進行 Win32 應用程式管理，但僅限Intune客戶對於其 Win32 應用程式會有更大的管理功能。本主題提供 Intune Win32 應用程式管理功能和相關資訊的概觀。

NOTE

此應用程式管理功能支援適用於 Windows 應用程式的 32 位和 64 位作業系統架構。

IMPORTANT

當您部署 Win32 應用程式時，請考慮以獨佔方式使用[Intune 管理延伸](#)模組方法，特別是當您有多個檔案的 Win32 應用程式安裝程式時。如果您在 Autopilot 註冊期間混合安裝 Win32 應用程式和企業營運應用程式，應用程式安裝可能會失敗，因為兩者同時使用信任的安裝程式服務。

將 PowerShell 腳本或 Win32 應用程式指派給使用者或裝置時，會自動安裝Intune管理延伸模組。此外，Intune管理延伸模組代理程式會每小時檢查 (或在服務或裝置重新開機時) 是否有任何新的 Win32 應用程式指派。

先決條件

若要使用 Win32 應用程式管理，請確定符合下列準則：

- 使用 Windows 10 1607 版或更新版本 (Enterprise、Pro 或 Education 版本)。
- 裝置必須註冊于Intune和下列其中一種：
 - [已註冊 Azure AD](#)
 - [已加入 Azure AD](#)
 - [已使用混合式 Azure AD 而聯結的](#)
- 每個應用程式的 Windows 應用程式大小不得大於 8 GB。

NOTE

如果 PowerShell 腳本或 Win32 應用程式是以使用者或裝置為目標，Intune會自動在裝置上安裝Intune管理延伸模組 (IME)。

準備 Win32 應用程式內容以上傳

您必須先使用 Microsoft Win32 內容準備工具來準備應用程式，才能將 Win32 應用程式新增至Microsoft Intune。您可以使用 Microsoft Win32 內容準備工具預先處理 Windows 傳統 (Win32) 應用程式。此工具會將應用程式安裝檔案轉換成 *.intunewin* 格式。如需詳細資訊和步驟，請 [參閱準備 Win32 應用程式內容以上傳](#)。

新增、指派及監視 Win32 應用程式

使用 Microsoft Win32 內容準備工具準備[Win32 應用程式上傳至Intune](#)之後，您可以將應用程式新增至Intune。如需詳細資訊和步驟，請參閱[在 Microsoft Intune 中新增、指派及監視 Win32 應用程式](#)。

NOTE

每個應用程式的 Windows 應用程式大小限制為 8 GB。

傳遞最佳化

Windows 10 1709 和更新版本的用戶端會使用 Windows 10 用戶端上的傳遞優化元件，下載 Intune Win32 應用程式內容。傳遞優化提供預設開啟的點對點功能。

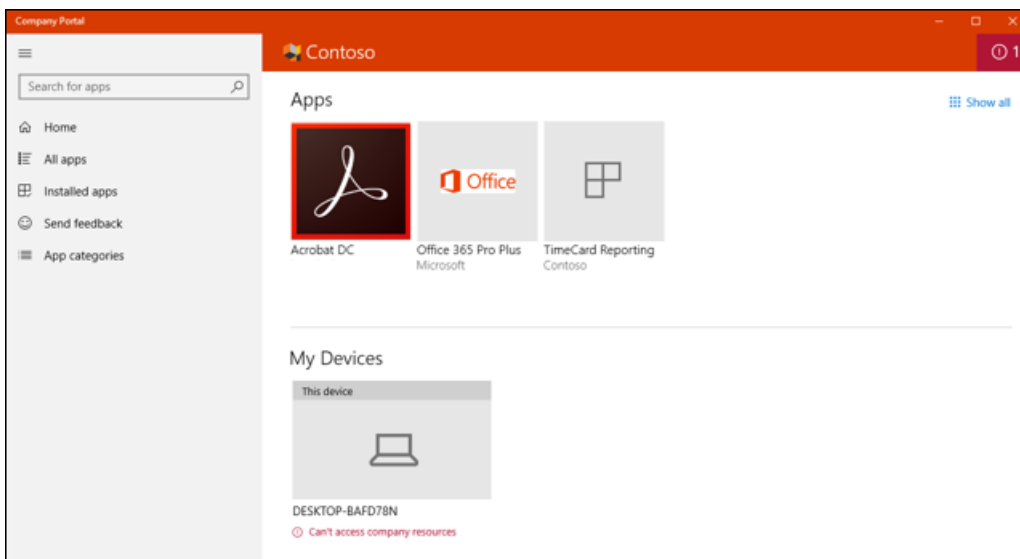
您可以設定傳遞優化代理程式，根據指派在背景或前景模式中下載 Win32 應用程式內容。傳遞優化可透過群組原則和裝置設定 Intune 來設定。如需詳細資訊，請參閱[Windows 10 的傳遞優化](#)。

NOTE

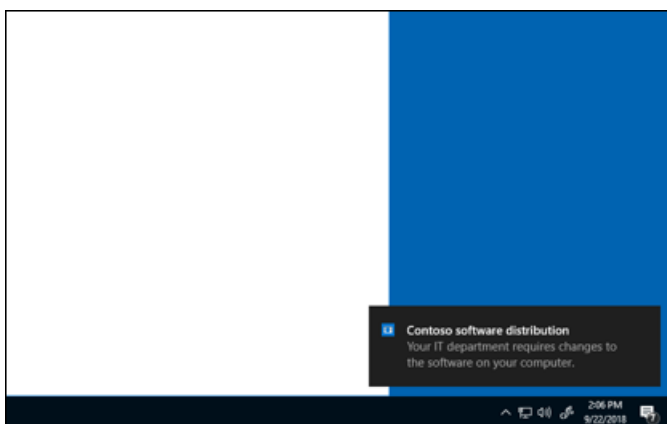
您也可以 Configuration Manager 發佈點上安裝 Microsoft 連線快取伺服器，以快取 Intune Win32 應用程式內容。如需詳細資訊，請參閱[microsoft Connected Cache in Configuration Manager](#)。

在裝置上安裝必要和可用的應用程式

使用者會看到必要和可用應用程式安裝的 Windows 通知。下圖顯示應用程式安裝在裝置重新開機之前未完成的範例通知。



下圖會通知使用者正在對裝置進行應用程式變更。



此外，公司入口網站應用程式會向使用者顯示更多應用程式安裝狀態訊息。下列條件適用於 Win32 相依性功能：

- 無法安裝應用程式。不符合系統管理員所定義的相依性。
- 應用程式已成功安裝，但需要重新開機。
- 應用程式正在安裝中，但需要重新開機才能繼續。

設定 Win32 應用程式可用性和通知

您可以設定 Win32 應用程式的開始時間和期限時間。在開始時，Intune 管理延伸模組會啟動應用程式內容下載，並針對必要意圖加以快取。應用程式將會在期限時間安裝。

針對可用的應用程式，開始時間會決定應用程式在公司入口網站中顯示的時間，而當使用者從公司入口網站要求應用程式時，將會下載內容。您也可以啟用重新開機寬限期。

IMPORTANT

只有當 [■] 區段的 [■] 設定為下列其中一個選項時，才能使用 [指 ■] 區段中的 [■] 設定：

- ■
- Intune■

使用下列步驟，根據所需應用程式的日期和時間設定應用程式可用性：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式] > [所有應用程式]。
3. 在 Windows 應用程式 (Win32) 清單中，選取應用程式。
4. 從應用程式窗格中，選取 [指派] 區段旁的 [屬性 > 編輯]。然後選取 [必要 指派類型] 下方的 [新增群組]。

請注意，您可以根據指派類型來設定應用程式可用性。指派類型 可以是 [必要]、[適用於已註冊的裝置] 或 [卸載]。

5. 在 [選取群組] 窗格上選取群組，以指定要指派應用程式的使用者群組。

NOTE

■ 選項包括下列各項：

- ■：您可以選擇 ■ 和/或 ■。
- ■：您可以選擇 ■。
- ■：您可以為 ■，以及/或卸 ■。

6. 若要修改 使用者通知 選項，請選取 [顯示所有快顯通知]。
7. 在 [編輯指派] 窗格中，將 [使用者通知] 設定為 [顯示所有快顯通知]。請注意，您可以將 使用者通知 設定為 [顯示所有快顯通知]、[顯示電腦重新開機的快顯通知] 或 [隱藏所有快顯通知]。
8. 將 [應用程式可用性] 設定為 [特定日期和時間]，然後選取您的日期和時間。此日期和時間會指定應用程式下載到使用者裝置的時間。
9. 將 [應用程式安裝期限] 設定為 [特定日期和時間]，然後選取您的日期和時間。這個日期和時間會指定應用程式安裝在使用者裝置上的時機。針對相同的使用者或裝置進行一個以上的指派時，會根據可能的最早時間挑選應用程式安裝期限時間。
10. 選取 [重新開機寬限期] 旁的 [啟用]。一旦裝置上的應用程式安裝完成，就會開始重新開機寬限期。停用設定時，裝置可以重新開機，而不會出現警告。

您可以自訂下列選項：

- **裝置重新開機寬限期 (分鐘)**：預設值為 1, 440 分鐘, (24 小時)。此值最多可以是 2 周。
- **選取在重新開機發生前顯示重新開機倒數計時對話方塊的時機 (分鐘)**：預設值為 15 分鐘。
- **允許使用者延遲重新開機通知**：您可以選擇 [是] 或 [否]。
 - **選取延遲持續時間 (分鐘)**：預設值為 240 分鐘 (4 小時)。延遲值不能超過重新開機寬限期。

11. 選取 [檢閱 + 儲存]。

Win32 應用程式的通知

如有需要，您可以隱藏顯示每個應用程式指派的使用者通知。從 [Intune]，選取 [應用程式 >][應用程式][應用程式 > >]*[指派 > 包含群組]。

NOTE

透過Intune管理延伸模組安裝的 Win32 應用程式不會在未註冊的裝置上卸載。系統管理員可以使用指派排除來不提供 Win32 應用程式，將您自己的裝置 (BYOD) 裝置。

後續步驟

- 如需將應用程式新增至Intune的詳細資訊，請參閱[將應用程式新增至Microsoft Intune](#)。

準備要上傳的 Win32 應用程式內容

2022/9/27 •

您必須先使用[Microsoft Win32 內容準備工具](#)來準備應用程式，才能將 Win32 應用程式新增至 Microsoft Intune。

必要條件

若要使用 Win32 應用程式管理，請確定您符合下列準則：

- 使用 Windows 10 版本1607或更新版本 (Enterprise、Pro 及教育版)。
- 裝置必須已註冊或加入 Azure Active Directory (Azure AD) 及自動註冊。Intune 管理擴充支援已註冊、Azure AD 加入、混合式網域加入的 Azure AD 裝置，以及已註冊的群組原則。

NOTE

針對群組原則註冊的情況，使用者會使用本機使用者帳戶來 Azure AD 加入其 Windows 10 裝置。使用者必須使用 Azure AD 使用者帳戶登入裝置，並在 Intune 註冊。如果 PowerShell 腳本或 Win32 應用程式是針對使用者或裝置，則 Intune 會在裝置上安裝 Intune 管理擴展。

- Windows 應用程式大小上限為每個應用程式 8 GB。

轉換 Win32 應用程式內容

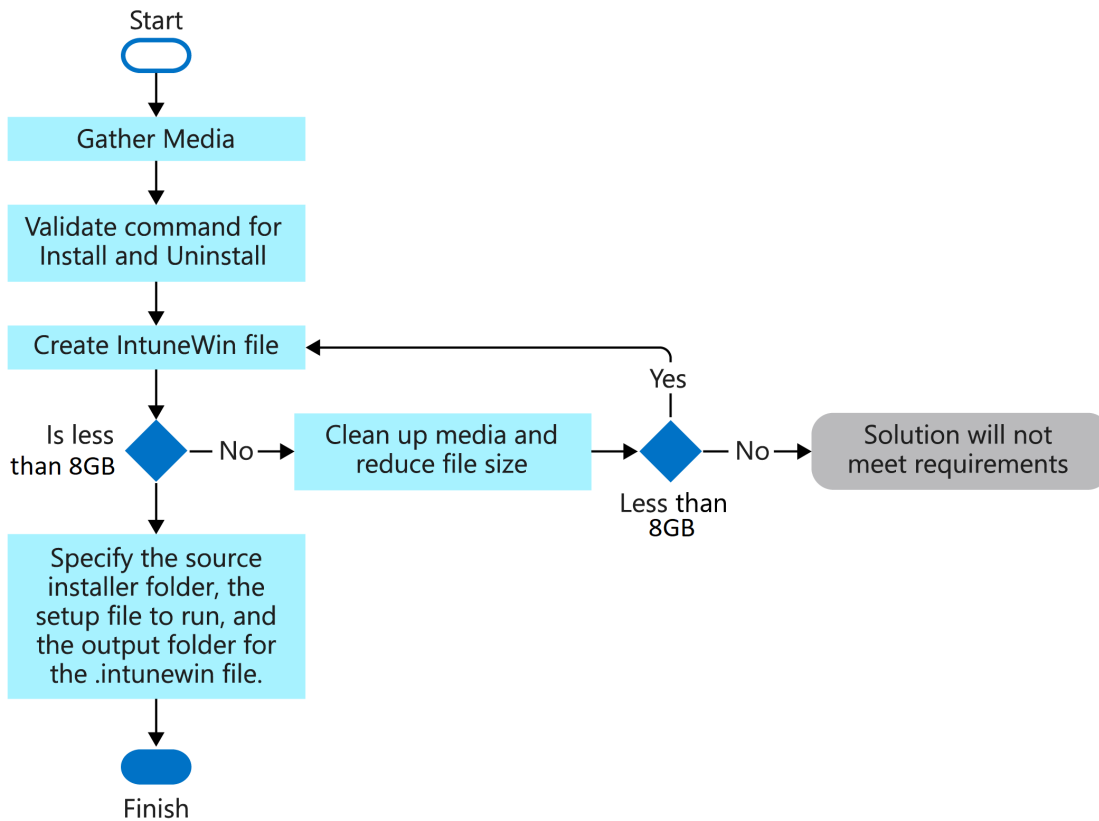
使用[Microsoft Win32 內容準備工具](#)，以預先處理 Windows 傳統 (Win32) 應用程式。工具會將應用程式安裝檔轉換為 *intunewin* 格式。工具也會偵測一些 Intune 需要判斷應用程式安裝狀態的屬性。在應用程式安裝程式資料夾上使用此工具後，您就可以在 Intune 主控台中建立 Win32 應用程式。

IMPORTANT

[Microsoft Win32 內容準備工具](#)會在建立 *intunewin* 檔案時，zips 所有的檔案與子資料夾。請務必保持 Microsoft Win32 內容準備工具與安裝程式檔案及資料夾分開，這樣您就不會在 *intunewin* 檔案中包含工具或其他不必要的檔案和資料夾。

您可以從 GitHub 下載[Microsoft Win32 內容準備工具](#)，將其當作 .zip 檔案。Zipped 檔案包含名為 Microsoft Win32 內容的資料夾，也就是 *準備工具-主* 圖形。資料夾包含準備工具、授權、讀我檔案和發行附注。

建立 intunewin 檔案的程式流程



執行 Microsoft Win32 內容準備工具

如果您從沒有參數的命令視窗中執行 `IntuneWinAppUtil.exe`，則工具會引導您輸入必要的參數逐步步驟。或者，您可以根據下列可用命令列參數，將參數新增至命令。

可用命令列參數

參數	說明
<code>-h</code>	說明
<code>-c <setup_folder></code>	所有安裝檔案的資料夾。此資料夾中的所有檔案都會壓縮為 <i>intunewin</i> 檔案。
<code>-s <setup_file></code>	安裝程式檔案 (例如 <i>setup.exe</i> 或 <i>setup.msi</i>)。
<code>-o <output_folder></code>	所產生的 <i>intunewin</i> 檔案的輸出檔案夾。
<code>-q</code>	安靜模式。

範例命令

命令	說明
<code>IntuneWinAppUtil -h</code>	此命令會顯示工具的使用狀況資訊。
<code>IntuneWinAppUtil -c c:\testapp\v1.0 -s c:\testapp\v1.0\setup.exe -o c:\testappoutput\v1.0 -q</code>	這個命令會從指定的來源資料夾及安裝檔案產生 <i>intunewin</i> 檔案。若為 MSI 安裝程式檔案，此工具將會取得 Intune 所需的資訊。如果 <code>-q</code> 已指定，命令將以安靜模式執行。如果輸出檔已存在，則會覆寫該檔案。此外，如果輸出檔案夾不存在，則會自動建立該資料夾。

當您正在產生 *intunewin* 檔案時，請將需要參照的任何檔案放入 `setup` 資料夾的子資料夾中。然後，使用相對路

徑參照所需的特定檔案。例如：

安裝程式來源資料夾：*c:\testapp\v1.0*

授權檔案：*c:\testapp\v1.0\licenses\license.txt*

使用相對路徑 *licenses\license.txt* 來參照 *license.txt* 檔。

後續步驟

- 將 Win32 應用程式新增至 [Microsoft Intune](#)

在 Microsoft Intune 中新增、指派及監視 Win32 應用程式

2022/9/27 •

使用 [Microsoft Win32 內容準備工具](#) 將 Win32 應用程式上傳至 Intune 之後，您可以將應用程式新增至 Intune。若要深入瞭解如何準備要上傳的 Win32 應用程式，請參閱 [準備 Win32 應用程式內容以上傳](#)。

先決條件

若要使用 Win32 應用程式管理，請確定您符合下列準則：

- 使用 Windows 10 1607 版或更新版本 (企業版、專業版和教育版)。
- 裝置必須加入或註冊至 Azure Active Directory (Azure AD) 並自動註冊。Intune 管理延伸模組支援已加入 Azure AD、已註冊 Azure AD、已加入混合式網域或已註冊群組原則的裝置。

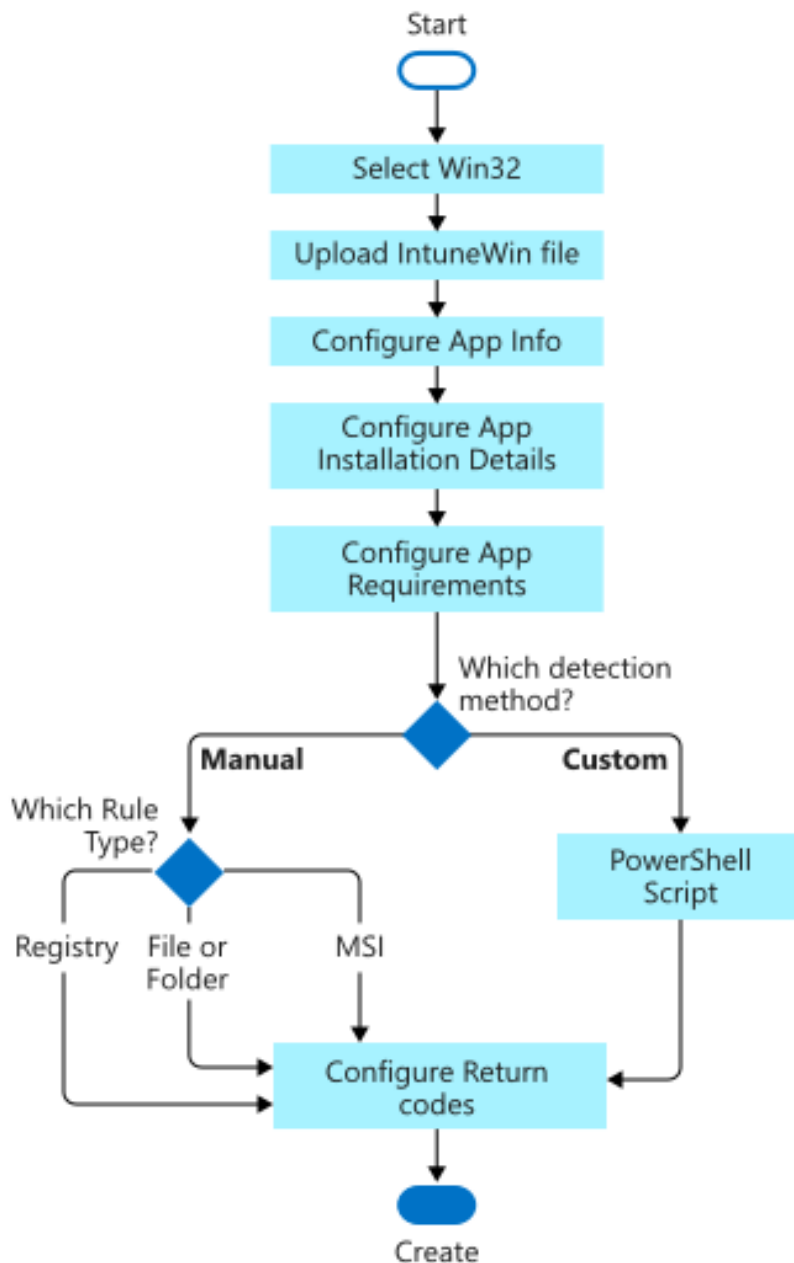
NOTE

針對群組原則註冊的案例，使用者會使用本機使用者帳戶來加入其 Windows 10 裝置的 Azure AD。使用者必須使用其 Azure AD 使用者帳戶登入裝置，並註冊 Intune。如果 PowerShell 腳本或 Win32 應用程式是以使用者或裝置為目標，Intune 會在裝置上安裝 Intune 管理擴充功能。

- 每個應用程式的 Windows 應用程式大小上限為 8 GB。

與標準企業營運 (LOB) 應用程式非常類似，您可以將 Win32 應用程式新增至 Microsoft Intune。這種類型的應用程式通常是由內部或由協力廠商撰寫。

將 Win32 應用程式新增至 Intune 的流程



將 Win32 應用程式新增至 Intune

下列步驟可協助您將 Windows 應用程式新增至 Intune：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式] > [新增]。
3. 在 [選取應用程式類型] 窗格的 [其他 應用程式類型] 底下，選取 [Windows 應用程式 (Win32)]。

IMPORTANT

請務必使用最新版的 Microsoft Win32 內容準備工具。如果您未使用最新版本，您會看到警告，指出已使用舊版工具封裝應用程式。

4. 按一下 [選取]。[新增應用程式] 步驟隨即出現。

步驟 1: 應用程式資訊

選取應用程式套件檔案

1. 在 [新增應用程式] 窗格中，按一下 [選取應用程式套件檔案]。
2. 在 [應用程式套件檔案] 窗格中，選取瀏覽按鈕。然後，選取副檔名為 *.intunewin* 的 Windows 安裝檔案。應用程式詳細資料隨即出現。
3. 當您完成時，請在 [應用程式套件檔案] 窗格上選取 [確定]。

設定應用程式資訊

在 [應用程式資訊] 頁面上，新增應用程式的詳細資料。視您選擇的應用程式而定，此頁面上的某些值可能會自動填入。

- **名稱**：輸入出現在公司入口網站中的應用程式名稱。請確定您使用的所有應用程式名稱都是唯一的。如果相同的應用程式名稱存在兩次，公司入口網站中只會出現其中一個應用程式。
- **描述**：輸入應用程式的描述。描述會出現在公司入口網站中。
- **發行者**：輸入應用程式的發行者名稱。
- **類別**：選取一或多個內建應用程式類別，或選取您所建立的類別。類別可讓使用者在流覽公司入口網站時更容易找到應用程式。
- **在公司入口網站中將此顯示為精選應用程式**：當使用者流覽應用程式時，在公司入口網站的主頁面上以醒目方式顯示應用程式。
- **資訊 URL**：選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會出現在公司入口網站中。
- **隱私權 URL**：選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會出現在公司入口網站中。
- **開發人員**：選擇性地輸入應用程式開發人員的名稱。
- **擁有者**：選擇性地輸入此應用程式擁有者的名稱。其中一個範例是 **人力資源部門**。
- **附注**：輸入您想要與此應用程式相關聯的任何附注。
- **標誌**：上傳與應用程式相關聯的圖示。當使用者流覽公司入口網站時，此圖示會與應用程式一起顯示。

選取 [下一步] 以顯示 [程式] 頁面。

步驟 2: 程式

在 [程式] 頁面上，設定應用程式的應用程式安裝和移除命令：

- **安裝命令**：新增完整的安裝命令列以安裝應用程式。

例如，如果您應用程式的檔案名是 **MyApp123**，請新增下列專案：

```
msiexec /p "MyApp123.msp"
```

如果應用程式為 `ApplicationName.exe`，則命令會是應用程式名稱，後面接著命令引數，(套件支援的) 切換。例如：

```
ApplicationName.exe /quiet
```

在上述命令中 `ApplicationName.exe`，封裝支援命令自 `/quiet` 變數。

如需應用程式套件支援的特定引數，請連絡您的應用程式廠商。

IMPORTANT

系統管理員在使用命令工具時必須小心。可能透過 [■] ■ 和 [■] ■ 欄位傳遞非預期或有害的命令。

- **卸載命令**：新增完整的命令列，以根據應用程式的 GUID 卸載應用程式。

例如：

```
msiexec /x "{12345A67-89B0-1234-5678-000001000000}"
```

- **安裝行為**：將安裝行為設定為 [系統] 或 [使用者]。

NOTE

您可以設定要安裝在 **■** 或 **■** 內容中的 Win32 應用程式。**■** 內容只指特定使用者。**■** 內容是指 Windows 10 裝置的所有使用者。

註冊 Azure AD 註冊裝置時，請選取 **[■]**。

使用者不需要登入裝置即可安裝 Win32 應用程式。

當應用程式設定為在使用者內容中安裝，且裝置上的使用者具有系統管理員許可權時，預設會在系統管理員許可權（下進行 Win32 應用程式安裝和卸載）。

- **裝置重新開機行為：**選取下列其中一個選項：
 - **根據傳回碼判斷行為：**選擇此選項以根據傳回碼重新開機裝置。此選項表示裝置會根據設定的傳回碼重新開機。使用此設定時，硬式重新開機傳回碼會立即觸發裝置的重新開機，而軟式重新開機傳回碼會通知使用者需要重新開機才能完成安裝。
 - **沒有特定動作：**選擇此選項可在 MSI 型應用程式的應用程式安裝期間抑制裝置重新開機。
 - **應用程式安裝可能會強制裝置重新開機：**選擇此選項可讓應用程式安裝完成，而不會抑制重新開機。此選項表示允許 Win32 應用程式安裝完成，而不會抑制重新開機。使用此設定時，硬式重新開機傳回碼會通知使用者裝置的重新開機將在 120 分鐘內觸發，而軟式重新開機傳回碼會通知使用者需要重新開機才能完成安裝。
 - **Intune 會強制裝置重新開機：**選擇此選項一律會在應用程式安裝成功之後重新開機裝置。
- **指定傳回碼以指出安裝後行為：**新增用來指定應用程式安裝重試行為或安裝後行為的傳回碼。根據預設，會在應用程式建立期間新增傳回碼專案。不過，您可以新增更多傳回碼或變更現有的傳回碼。
 1. 在 **[程式碼類型]** 資料行中，將 **[程式碼類型]** 設定為下列其中一項：
 - **失敗：**指出應用程式安裝失敗的傳回值。
 - **硬式重新開機：**硬式重新開機傳回碼不允許在用戶端上安裝下一個 Win32 應用程式，而不需重新開機。
 - **軟式重新開機：**軟式重新開機傳回碼可讓您安裝下一個 Win32 應用程式，而不需要重新開機用戶端。若要完成目前應用程式的安裝，必須重新開機。
 - **重試：**重試傳回碼代理程式會嘗試安裝應用程式三次。每次嘗試之間會等候五分鐘。
 - **成功：**指出應用程式已成功安裝的傳回值。
 2. 如有需要，請選取 **[新增]** 以新增更多傳回碼，或修改現有的傳回碼。

選取 **[下一步]** 以顯示 **[需求]** 頁面。

步驟 3: 需求

在 **[需求]** 頁面上，指定安裝應用程式之前裝置必須符合的需求：

- **作業系統架構：**選擇安裝應用程式所需的架構。
- **最低作業系統：**選取安裝應用程式所需的最低作業系統。
- **(MB) 所需的磁碟空間：**選擇性地新增系統磁片磁碟機上安裝應用程式所需的可用磁碟空間。
- **(MB) 所需的實體記憶體：**選擇性地新增安裝應用程式所需的實體記憶體 (RAM)。
- **所需的邏輯處理器數目下限：**選擇性地新增安裝應用程式所需的最小邏輯處理器數目。
- **MHz) (所需的最小 CPU 速度：**選擇性地新增安裝應用程式所需的最小 CPU 速度。
- **設定其他需求規則：**
 1. 選取 **[新增]** 以顯示 **[新增需求規則]** 窗格，並設定更多需求規則。選取 **[需求類型]** 值，以選擇您將用來判斷如何驗證需求的規則類型。需求規則可以根據檔案系統資訊、登錄值或 PowerShell 腳本。
 - **檔案：**當您選擇 **[檔案]** 作為 **[需求類型]** 值時，需求規則必須偵測檔案或資料夾、日期、版本或大小。

- **路徑**: 包含要偵測之檔案或資料夾的資料夾完整路徑。
- **檔案或資料夾**: 要偵測的檔案或資料夾。
- **屬性**: 選取用來驗證應用程式是否存在的規則類型。
- **與 64 位用戶端上的 32 位應用程式相關聯**: 選取 [是] 以展開 64 位用戶端上 32 位內容中的任何路徑環境變數。選取 [否 (預設)], 以展開 64 位用戶端上 64 位內容中的任何路徑變數。32 位用戶端一律會使用 32 位內容。
- **登錄**: 當您選擇 [登錄] 作為 [需求類型] 值時, 需求規則必須根據值、字串、整數或版本來偵測登錄設定。
 - **機碼路徑**: 包含要偵測之值的登錄專案完整路徑。
 - **值名稱**: 要偵測的登錄值名稱。如果此值是空的, 則會在索引鍵上進行偵測。如果偵測方法不是檔案或資料夾存在, 則金鑰的 (預設) 值會當做偵測值使用。
 - **登錄機碼需求**: 選取用來判斷如何驗證需求規則的登錄機碼比較類型。
 - **與 64 位用戶端上的 32 位應用程式相關聯**: 選取 [是] 以搜尋 64 位用戶端上的 32 位登錄。選取 [無 (預設)], 在 64 位用戶端上搜尋 64 位登錄。32 位用戶端一律會搜尋 32 位登錄。
- **腳本**: 當您無法根據檔案、登錄或Intune主控台中可用的任何其他方法建立需求規則時, 請選擇 [腳本] 作為 [需求類型] 值。
 - **腳本檔案**: 針對以 PowerShell 腳本需求為基礎的規則, 如果現有的程式碼為 0, 我們會更詳細地偵測 STDOUT) (標準輸出。例如, 我們可以將 STDOUT 偵測為值為 1 的整數。
 - **在 64 位用戶端上以 32 位進程執行腳本**: 選取 [是] 以在 64 位用戶端的 32 位進程中執行腳本。選取 [無 (預設)], 在 64 位用戶端的 64 位進程中執行腳本。32 位用戶端會在 32 位進程中執行腳本。
 - **使用登入的認證執行此腳本**: 選取 [是] 以使用已登入的裝置認證來執行腳本。
 - **強制執行腳本簽章檢查**: 選取 [是] 以確認信任的發行者已簽署腳本, 這可讓腳本執行, 而不會顯示警告或提示。腳本會解除封鎖執行。選取 [無 (預設)], 以在使用者確認的情況下執行腳本, 而不需要簽章驗證。
 - **選取輸出資料類型**: 選取用來判斷需求規則相符的資料類型。

2. 當您完成設定需求規則時, 請選取 [確定]。

選取 [下一步] 以顯示 [偵測規則] 頁面。

步驟 4: 偵測規則

在 [偵測規則] 窗格上, 設定規則以偵測應用程式是否存在。您可以選擇新增多個規則:

- **規則格式**: 選取如何偵測應用程式是否存在。您可以選擇手動設定偵測規則, 或使用自訂腳本來偵測應用程式是否存在。您必須至少選擇一個偵測規則。

NOTE

必須符合 所有 規則的條件, 才能偵測應用程式。

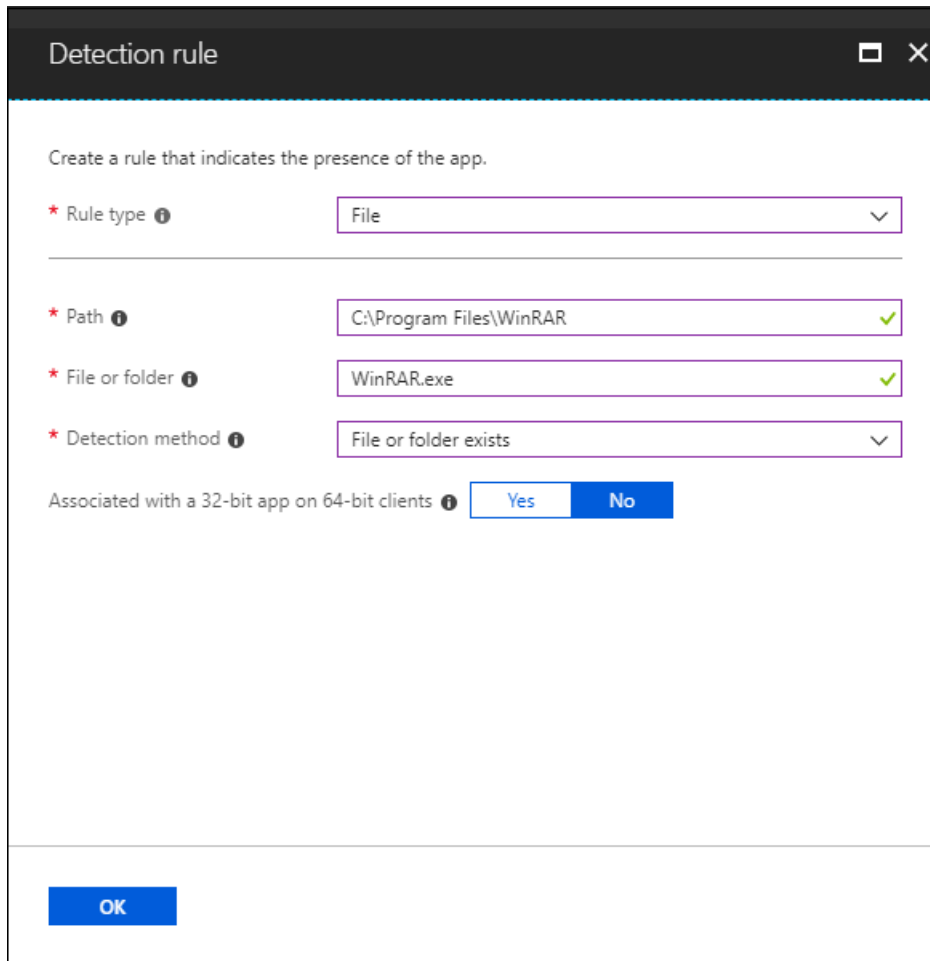
如果Intune偵測到裝置上沒有應用程式, Intune會在大約 24 小時內再次提供應用程式。這只會發生在以必要意圖為目標的應用程式。

- **手動設定偵測規則**: 您可以選取下列其中一種規則類型:
 - **MSI**: 根據 MSI 版本檢查進行驗證。此選項只能新增一次。當您選擇此規則類型時, 您有兩個設定:
 - **MSI 產品代碼**: 為應用程式新增有效的 MSI 產品代碼。
 - **MSI 產品版本檢查**: 選取 [是] 以驗證 MSI 產品版本以及 MSI 產品代碼。

- **檔案**：根據檔案或資料夾偵測、日期、版本或大小進行驗證。
 - **路徑**：輸入包含要偵測之檔案或資料夾的資料夾完整路徑。這不應該包含特殊字元，例如 `&`、`<` 或 `>`。
 - **檔案或資料夾**：輸入要偵測的檔案或資料夾。
 - **偵測方法**：選取用來驗證應用程式是否存在的偵測方法類型。
 - **與 64 位用戶端上的 32 位應用程式相關聯**：選取 [是] 以展開 64 位用戶端上 32 位內容中的任何路徑環境變數。選取 [否 (預設)]，以展開 64 位用戶端上 64 位內容中的任何路徑變數。32 位用戶端一律會使用 32 位內容。

檔案型偵測的範例

檢查檔案是否存在。



Detection rule

Create a rule that indicates the presence of the app.

* Rule type ⓘ File

* Path ⓘ C:\Program Files\WinRAR ✓

* File or folder ⓘ WinRAR.exe ✓

* Detection method ⓘ File or folder exists

Associated with a 32-bit app on 64-bit clients ⓘ Yes No

OK

檢查資料夾是否存在。

Detection rule

Create a rule that indicates the presence of the app.

* Rule type ⓘ File

* Path ⓘ C:\Program Files ✓

* File or folder ⓘ WinRAR ✓

* Detection method ⓘ File or folder exists

Associated with a 32-bit app on 64-bit clients ⓘ Yes No

OK

- **登錄**：根據值、字串、整數或版本進行驗證。
 - **機碼路徑**：包含要偵測之值的登錄專案完整路徑。有效的語法為 HKEY_LOCAL_MACHINE\Software\WinRAR 或 HKLM\Software\WinRAR。
 - **值名稱**：要偵測的登錄值名稱。如果此值是空的，則會在索引鍵上進行偵測。如果偵測方法不是檔案或資料夾存在，則金鑰的 (預設) 值會當做偵測值使用。
 - **偵測方法**：選取用來驗證應用程式存在的偵測方法類型。
 - **與 64 位用戶端上的 32 位應用程式相關聯**：選取 [是] 以搜尋 64 位用戶端上的 32 位登錄。選取 [無 (預設)]，在 64 位用戶端上搜尋 64 位登錄。32 位用戶端一律會搜尋 32 位登錄。

登錄型偵測的範例

檢查登錄機碼是否存在。

Detection rule

Create a rule that indicates the presence of the app.

* Rule type ⓘ

Registry

* Key path ⓘ

HKEY_LOCAL_MACHINE\SOFTWARE\WinRAR

Value name ⓘ

* Detection method ⓘ

Key exists

Associated with a 32-bit app on 64-bit clients ⓘ

Yes

No

OK

檢查登錄值是否存在。

Detection rule

Create a rule that indicates the presence of the app.

* Rule type ⓘ

Registry

* Key path ⓘ

HKEY_LOCAL_MACHINE\SOFTWARE\WinRAR

Value name ⓘ

exe64

* Detection method ⓘ

Value exists

Associated with a 32-bit app on 64-bit clients ⓘ

Yes

No

OK

檢查登錄值字串是否相等。

Detection rule

Create a rule that indicates the presence of the app.

* Rule type Registry

* Key path HKEY_LOCAL_MACHINE\SOFTWARE\WinRAR ✓

Value name exe64

* Detection method String comparison

* Operator Equals

* Value C:\Program Files\WinRAR\WinRAR.exe ✓

Associated with a 32-bit app on 64-bit clients

- **使用自訂偵測腳本：**指定將用來偵測此應用程式的 PowerShell 腳本。
 - **腳本檔案：**選取 PowerShell 腳本，以偵測用戶端上的應用程式是否存在。當腳本同時傳回 0 值結束代碼，並將字串值寫入 STDOUT 時，將會偵測到應用程式。
 - **在 64 位用戶端上以 32 位進程執行腳本：**選取 [是] 以在 64 位用戶端的 32 位進程中執行腳本。選取 [無 (預設)]，在 64 位用戶端的 64 位進程中執行腳本。32 位用戶端會在 32 位進程中執行腳本。
 - **強制執行腳本簽章檢查：**選取 [是] 以確認信任的發行者已簽署腳本，這可讓腳本執行，而不會顯示警告或提示。腳本會解除封鎖執行。選取 [無 (預設)]，在沒有簽章驗證的情況下執行腳本。

Intune 代理程式會檢查腳本的結果。它會讀取腳本寫入 STDOUT 資料流程的值、STDERR) 資料流程 (標準錯誤，以及結束代碼。如果腳本以非零值結束，腳本會失敗，且未安裝應用程式偵測狀態。如果結束代碼為零且 STDOUT 有資料，則會安裝應用程式偵測狀態。

NOTE

建議您將腳本編碼為 UTF-8。當腳本結束且值為 0 時，腳本執行會成功。第二個輸出通道指出已偵測到應用程式。STDOUT 資料表示在用戶端上找到應用程式。我們不會從 STDOUT 尋找特定字串。

您的 Win32 應用程式版本會顯示在 Microsoft 端點管理員 系統管理中心。應用程式版本會在 [所有應用程式] 清單中提供，您可以在其中依 Win32 應用程式進行篩選，然後選取選擇性 版本資料行。在 [Microsoft 端點管理員 系統管理中心](#)，選取 [應用程式 > 所有應用程式 > > 資料行 版本] 以在應用程式清單中顯示應用程式版本。

新增規則之後，請選取 [下一步] 以顯示 [相依性] 頁面。

步驟 5: 相依性

應用程式相依性是必須先安裝，才能安裝 Win32 應用程式的應用程式。您可以要求將其他應用程式安裝為相依

性。

具體而言，裝置必須先安裝相依應用程式，才能安裝 Win32 應用程式。最多 100 個相依性，包括任何包含相依性的相依性，以及應用程式本身。

您只能在 Win32 應用程式新增並上傳至Intune之後，才新增 Win32 應用程式相依性。新增 Win32 應用程式之後，您會在 Win32 應用程式的窗格上看到 [相依性] 選項。

任何 Win32 應用程式相依性也必須是 Win32 應用程式。它不支援視其他應用程式類型而定，例如單一 MSI LOB 應用程式或 Microsoft Store 應用程式。

當您新增應用程式相依性時，可以根據應用程式名稱和發行者進行搜尋。此外，您可以根據應用程式名稱和發行者來排序新增的相依性。您無法在新增的應用程式相依性清單中選取先前新增的應用程式相依性。

您可以選擇是否要自動安裝每個相依應用程式。根據預設，每個相依性都會將 [自動安裝] 選項設定為 [是]。自動安裝相依應用程式，即使相依應用程式不是以使用者或裝置為目標，Intune也會在裝置上安裝應用程式，以滿足相依性，再安裝您的 Win32 應用程式。

NOTE

如果應用程式是以使用者或裝置為目標，則相依應用程式的安裝狀態會顯示在Intune內。

請務必注意，相依性可以有遞迴子相依性，而且在安裝主要相依性之前，會先安裝每個子相依性。此外，相依性的安裝不會遵循相依性層級的特定順序。

新增到Intune的 Win32 應用程式在相依性關聯性時無法移除。只有在移除相依性關聯性之後，才能刪除這些應用程式。這項需求會同時套用至相依性關聯性中的父應用程式和子應用程式。此外，這項需求可確保正確強制執行相依性，而且相依性行為更容易預測。

選取相依性

在 [相依性] 頁面上，選取必須先安裝才能安裝 Win32 應用程式的應用程式：

1. 選取 [新增] 以顯示 [新增相依性] 窗格。
2. 新增相依應用程式，然後按一下 [選取]。
3. 在 [自動安裝] 資料行下選取 [是] 或 [否]，選擇是否要自動安裝相依應用程式。

選取相依性之後，請選取 [下一步] 以顯示 [範圍標籤] 頁面。

瞭解其他相依性詳細資料

使用者會看到 Windows 通知，指出相依應用程式正在下載並安裝為 Win32 應用程式安裝程式的一部分。

相依性限制

下列項目符號清單提供相依性限制的其他明確性：

- 如果應用程式有 100 個相依性，則應用程式圖形的大小總計為 101 (100 個相依性應用程式 + 1 個父應用程式)。
- 如果應用程式有 3 個相依性，而且其中一個相依性應用程式有 2 個相依性，則應用程式圖形的大小總計為 6 (1 個父應用程式 + 3 個相依性應用程式 + 2 個相依性應用程式來自另一個相依性應用程式)。
- 如果應用程式是多個應用程式「圖形」的相依性，表示相依性位於某些應用程式圖形的相依性鏈結中，則所有不同圖形中的所有應用程式都會加總以計算相依性大小。例如，如果圖形 A 有 23 個應用程式、圖形 B 有 62 個應用程式，而圖形 C 有 20 個應用程式，而 app X 在所有 3 個圖形的相依性鏈結中某處存在為相依性應用程式，則圖表的大小總計為 103 (應用程式 X 只會計算一次)，這超過 100 個限制限制。

相依性失敗

未安裝相依應用程式時，使用者通常會看到下列其中一個通知：

- 無法安裝一或多個相依應用程式。

- 不符合一或多個相依應用程式需求。
- 一或多個相依應用程式正在等待裝置重新開機。

如果您選擇不要在 [自動安裝] 資料行中放置相依性，則不會嘗試安裝 Win32 應用程式。此外，應用程式報告會顯示相依性已標示為 `failed`，並提供失敗原因。您可以選取 Win32 應用程式安裝詳細資料中提供的失敗 (或警告) 來檢視相依性 **安裝** 失敗。

每個相依性都會遵守 Intune Win32 應用程式重試邏輯 (在等候五分鐘之後嘗試安裝三次，) 和全域重新評估排程。此外，相依性僅適用於在裝置上安裝 Win32 應用程式時。相依性不適用於卸載 Win32 應用程式。若要刪除相依性，您必須選取相依性清單資料列結尾的相依應用程式左邊 (三個點) 省略號。

步驟 6: 取代

NOTE

Win32 應用程式取代處於公開預覽狀態。

當您取代應用程式時，可以指定要更新或取代的應用程式。若要更新應用程式，請停用卸載舊版選項。若要取代應用程式，請啟用卸載舊版選項。最多有 10 個更新或取代的應用程式，包括其他應用程式的參考。例如，您的應用程式會參考另一個應用程式。這個其他應用程式會參考其他應用程式，依此類推。此案例會建立應用程式的圖形。圖形中的所有應用程式都會計入最大值 10。

若要新增目前應用程式將取代的應用程式：

1. 在 [取代] 步驟中，按一下 [新增] 以選擇應該取代的應用程式。

NOTE

在 Intune 中，取代關聯性中最多可以有 10 個節點。

2. 在 [新增 應用程式] 窗格中尋找並按一下應用程式以套用取代關聯性。按一下 [選取] 將應用程式新增至取代清單。
3. 在已取代的應用程式清單中，針對每個選取的應用程式修改 [卸載舊版] 選項，以指定 Intune 是否要將卸載命令傳送至每個選取的應用程式。如果目前應用程式的安裝程式自動更新選取的應用程式，則不需要傳送卸載命令。將選取的應用程式取代為不同的應用程式時，可能需要開啟 [卸載舊版] 選項，以移除並取代繼承應用程式。
4. 完成此步驟之後，按 [下一步]。

如需詳細資訊，請 [參閱新增 Win32 應用程式取代](#)。

步驟 7: 指派

您可以選取 [必要]、[適用於已註冊的裝置] 或 [卸載 應用程式的群組指派]。如需詳細資訊，請 [參閱新增群組以組織使用者和裝置](#) 和 [使用 Microsoft Intune 將應用程式指派給群組](#)。

IMPORTANT

針對根據使用者目標部署和指派 Win32 應用程式的案例，如果 Win32 應用程式需要裝置系統管理員許可權或裝置的標準使用者沒有的任何其他許可權，則應用程式將無法安裝。

1. 針對特定應用程式，選取指派類型：
 - **必要**：應用程式會安裝在所選群組中的裝置上。

- **適用於已註冊的裝置**：使用者可從公司入口網站應用程式或公司入口網站安裝應用程式。
 - **卸載**：應用程式會從所選群組中的裝置卸載。
2. 選取 **[新增群組]**，然後指派將使用此應用程式的群組。
 3. 在 **[選取群組]** 窗格中，選取要根據使用者或裝置指派的群組。
 4. 選取群組之後，您也可以設定 **使用者通知、可用性和****安裝期限**。如需詳細資訊，請 [參閱設定 Win32 應用程式可用性和通知](#)。
 5. 如果您不想讓此應用程式指派影響使用者群組，請選取 [MODE] 資料行下的 **[包含]**。在 **[編輯指派]** 窗格中，將 **模式** 值從 **[包含]** 變更為 **[排除]**。選取 **[確定]** 以關閉 **[編輯指派]** 窗格。
 6. 在 **[應用程式設定]** 區段中，選取應用程式的 **[傳遞優化優先順序]** 值。此設定將決定應用程式內容的下載方式。您可以選擇根據指派，在背景模式或前景模式中下載應用程式內容。

完成應用程式的指派設定之後，選取 **[下一步]** 以顯示 **[檢閱 + 建立]** 頁面。

步驟 8: 檢閱和建立

1. 檢閱您為應用程式輸入的值和設定。確認您已正確設定應用程式資訊。
2. 選取 **[建立]** 將應用程式新增至 [Intune]。

LOB 應用程式的 **[概觀]** 窗格隨即出現。

此時，您已完成將 Win32 應用程式新增至 Intune 的步驟。如需應用程式指派和監視的相關資訊，請參閱[使用 Microsoft Intune將應用程式指派給群組和使用Microsoft Intune監視應用程式資訊和指派](#)。

後續步驟

- [使用 Microsoft Intune 監視應用程式資訊和指派](#)
- [針對 Win32 應用程式問題進行疑難排解](#)

新增 Win32 應用程式取代

2022/9/27 •

NOTE

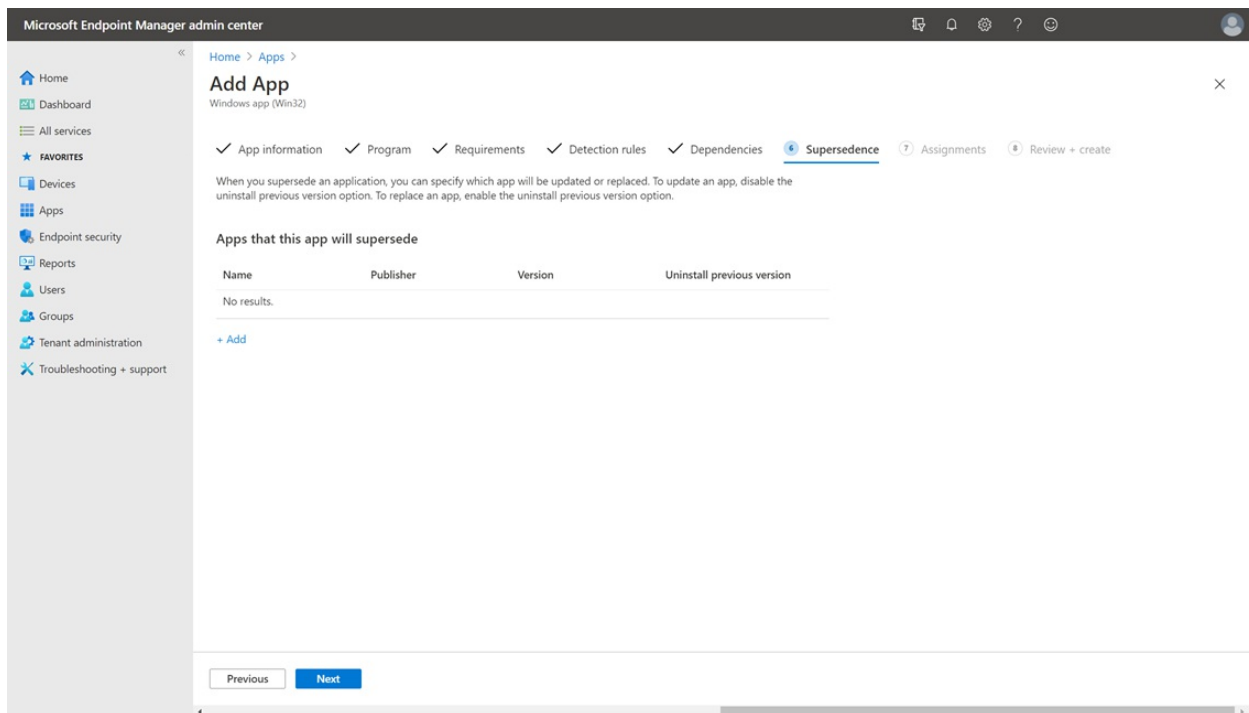
Win32 應用程式取代處於公開預覽狀態。

將[Win32 應用程式新增至Intune](#)之後，您可以使用Intune在應用程式之間建立一或多個取代關聯性。一般而言，取代是您更新或取代某個專案的地方。在Intune中，取代可讓您以相同應用程式或完全不同的 Win32 應用程式較新版本來更新和取代現有的 Win32 應用程式。本主題提供取代功能的概觀。

IMPORTANT

取代可讓您更新和取代 Win32 應用程式的版本，目前不允許您將 Win32 應用程式與應用程式相依性交換。如需應用程式相依性的詳細資訊，請參閱 [相依性](#)。

在Intune內新增或修改 Win32 應用程式時，可以建立取代關聯性。**取代** 步驟可讓您指定與 Win32 應用程式相關的任何取代關聯性。



先決條件

應用程式取代只能套用至 Win32 應用程式。如需詳細資訊，請參閱將[Win32 應用程式新增至Intune](#)。

需要 Microsoft 端點管理員 許可權，才能建立和編輯 Win32 應用程式與其他應用程式的取代和相依性關聯性。選取 [關聯]，即可在 [行動應用程式] 類別下取得權限。從 2202 服務版本開始，MEM 系統管理員在 Microsoft 端點管理員 系統管理中心建立或編輯 Win32 應用程式時，需要此許可權才能新增取代和相依性應用程式。若要在 [Microsoft 端點管理員 系統管理中心](#) 尋找此許可權，請選擇 [租使用者系統管理 > 角色 >][所有角色 > 建立]。

此 Win32 應用程式取代許可權已新增至下列內建角色：

- 應用程式管理員
- 學校系統管理員

在 Intune 中建立取代關聯性

下列步驟可協助您建立應用程式之間的取代關聯性：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式]，然後從清單中選取 Win32 應用程式。如果您尚未新增 Win32 應用程式，您可以依照步驟將[Win32 應用程式新增至Intune](#)。
3. 選取現有的 Win32 應用程式之後，按一下 [屬性]。
4. 在 [取代] 區段中，按一下 [編輯 > 新增] 以選擇應取代的應用程式。

NOTE

在Intune中，取代關聯性中最多可以有 10 個節點。

5. 在 [新增 應用程式] 窗格中尋找並按一下應用程式以套用取代關聯性。按一下 [選取] 將應用程式新增至取代清單。
6. 在已取代的應用程式清單中，針對每個選取的應用程式修改 [卸載舊版] 選項，以指定Intune是否要將卸載命令傳送至每個選取的應用程式。如果目前應用程式的安裝程式自動更新選取的應用程式，則不需要傳送卸載命令。將選取的應用程式取代為不同的應用程式時，可能需要開啟 [卸載舊版] 選項，以移除並取代繼承應用程式。
7. 完成此步驟之後，按一下 [檢閱 + 儲存 >]。

IMPORTANT

取代的應用程式不會自動取得目標。每個應用程式都必須有明確的目標才能生效。代理程式會忽略未設為目標的取代應用程式。如果取代的應用程式是以具有已取代應用程式的裝置為目標，則不論已取代的應用程式是否有目標，都會取代。如需取代行為的詳細資訊，請參閱下列矩陣。此行為與不需要目標的相依性直接對比。此外，只有目標應用程式才會在 Microsoft 端點管理員 系統管理中心顯示安裝狀態。

取代行為

取代的應用程式 是更新或取代其他應用程式的應用程式。*已取代的應用程式* 是正在更新或取代的應用程式。取代行為可以根據下列案例來說明。

“	““““““““	““““““““
■ 1： 已取代的應用程式存在於裝置上，而 [■ ■] 設定為 [■]。	已取代的應用程式將會卸載，而已取代的應用程式將會安裝在裝置上。 ■：即使已取代的應用程式不是目標，它還是會卸載。	只有取代的應用程式才會顯示在公司入口網站中，而且可以安裝。
■ 2： 已取代的應用程式存在於裝置上，而 [■ ■] 設定為 [■]。	取代的應用程式將會安裝在裝置上。是否要卸載已取代的應用程式，取決於已取代應用程式的安裝程式。	只有取代的應用程式才會顯示在公司入口網站中，而且可以安裝。
■ 3： 已取代的應用程式不存在於裝置上。	將會安裝取代的應用程式。	新的應用程式會出現在公司入口網站中。

瞭解應用程式更新與取代內的應用程式取代

假設應用程式可以有多个已取代的應用程式，應用程式可以同时更新一组應用程式，同时取代另一组應用程式。

NOTE

终端使用者将无法检查特定 Win32 應用程式取代作业是否为公司入口网站中的更新或取代。此外，当多个應用程式取代公司入口网站中具有可用目标的應用程式时，已取代應用程式的详细信息页面会浏览至已设定之第一个取代應用程式的應用程式页面。例如，如果應用程式 A 被應用程式 B 和 C 取代，而應用程式 B 先被應用程式 A 取代，则應用程式 A 在公司入口网站中的详细信息页面会浏览至應用程式 B。

您可以根据下列案例，说明更新應用程式與取代應用程式時如何套用取代。

更新或取代	更新或取代的應用程式	更新或取代的應用程式	更新或取代的應用程式
應用程式更新	IT 系統管理員想要使用相同應用程式的較新版本來更新應用程式。	新版應用程式的安裝程式 (取代的應用程式) 會自動將繼承應用程式更新為較新版本。	由於安裝程式將會完成更新，因此不需要將卸載命令傳送至舊版。因此，卸載舊版會關閉。
應用程式取代	IT 系統管理員想要以完全不同的應用程式取代應用程式。	將卸載已取代的應用程式，並安裝已取代的應用程式。安裝和卸載都會以 IT 專業人員定義的安裝/卸載命令列為基礎。	由於這兩個應用程式不同，系統管理員可以開啟 [卸載舊版] 切換，從裝置卸載較舊的應用程式。

瞭解就地應用程式更新與取代應用程式更新

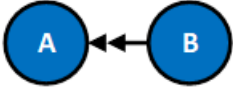
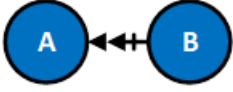
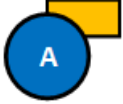
在下列案例中，您應該在執行下列任一種更新之後，檢閱應用程式偵測規則。

更新或取代	更新或取代的應用程式
就地應用程式更新	- 使用就地應用程式更新時，系統管理員只能交換應用程式內容、更新中繼資料，以及變更偵測和安裝命令。 - 管理員無法使用就地應用程式更新來變更未儲存在應用程式上的任何欄位。例如，系統管理員無法在更新的同時修改目標。 - 管理員一次只能執行一個應用程式的就地應用程式更新。
取代應用程式更新	- 管理員可以使用一組新的組態來完整更新應用程式。 - 管理員可以選擇關閉卸載命令，以卸載先前的應用程式版本。 - 管理員可以使用一個取代設定，將包含多個應用程式版本的裝置更新為最新的應用程式版本。系統管理員也會維護繼承應用程式的存取權。

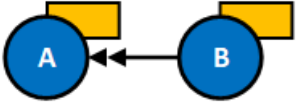
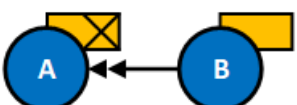
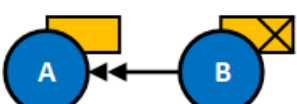
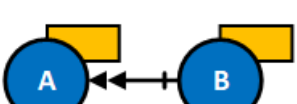
基本取代範例

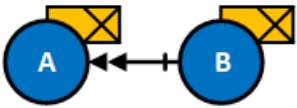
基於本檔的目的，我們假設所有應用程式都是以) 為目標的裝置或使用者 (目標，而且都適用。

取代範例案例的圖例

	B 會透過應用程式更新取代。
	B 會透過應用程式取代來取代。
	存在於裝置上、完整安裝，並通過定義的偵測規則。
	裝置上沒有。

案例和解決方法取代範例

	■：裝置上未偵測到任何應用程式。B 會透過應用程式更新取代。 ■：安裝 B。	應用程式更新表示系統管理員選擇不要在設定階段卸載已取代的應用程式。請參閱上方的應用程式部署中的取代步驟。
	■：裝置上只會偵測到 A。B 會透過應用程式更新取代。 ■：安裝 B。	由於系統管理員選擇不要在設定期間卸載舊版，因此Intune不會明確卸載 A。可能會根據 B 安裝程式的行為來卸載。
	■：裝置上只會偵測到 B。B 會透過應用程式更新取代。 ■：什麼。	由於已在裝置上偵測到 B，因此不會採取任何動作。
	■：這兩個應用程式都會在裝置上偵測到。B 會透過應用程式更新取代。 ■：什麼。	由於已在裝置上偵測到 B，因此不會採取任何動作。管理員在設定時選擇不要卸載舊版，因此不會卸載 A。
	■：裝置上未偵測到任何應用程式。B 會透過應用程式取代來取代。 ■：安裝 B。	應用程式取代表示系統管理員選擇在設定階段卸載已取代的應用程式。請參閱上方的應用程式部署中的取代步驟。
	■：裝置上只會偵測到 A。B 會透過應用程式取代來取代。 ■：卸載 A，然後安裝 B。	將會卸載，一旦代理程式偵測到 A 已不存在於裝置上，就會安裝 B。如果偵測持續偵測到 A 是否存在，則代理程式將不會安裝 B。是否在裝置上安裝 B 是以裝置上是否偵測到 A 作為述詞。
	■：裝置上只會偵測到 B。B 會透過應用程式取代來取代。 ■：沒有	因為 B 已安裝，且 A 不存在於裝置上，所以不會採取任何動作。

II	IIII	II
	■：這兩個應用程式都會在裝置上偵測到。B 會透過應用程式取代來取代。 ■：卸載 A。	會在應用程式取代程式中卸載。在已安裝取代應用程式之後偵測已取代的應用程式，將會強制執行補救。

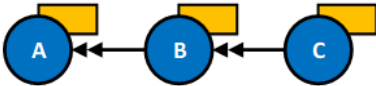
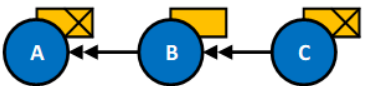
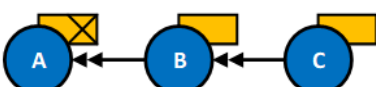
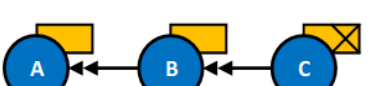
鏈結式取代案例的行為

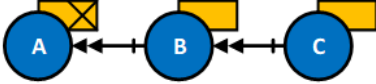
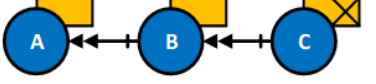
當多個應用程式屬於取代關聯性時，就會發生取代鏈結。例如，IT 系統管理員可以將應用程式 A 設定為由應用程式 B 取代，然後設定 App B 以由 App C 取代。在此案例中，應用程式 A、B 和 C (之間會建立取代鏈結，如下) 的第一個案例所示。取代鏈結在鏈結中最多可以有 10 個相關節點。如需此上限的詳細資訊，請參閱 [取代限制](#)。

取代鏈結的行為摘要如下：

- 取代鏈結中的所有應用程式都會被鏈結的取代應用程式取代。在上述範例中，鏈結的取代應用程式是 App C。

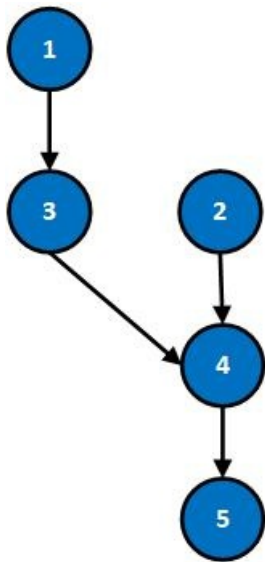
為了進一步瞭解取代鏈結的行為，下表提供案例和解決方法的清單。檢閱這些取代鏈結時，假設所有應用程式都是目標，且適用於裝置。

II	IIII	II
	■：裝置上沒有任何應用程式存在。應用程式之間的關聯性是其中一個應用程式更新。 ■：安裝 C。	由於裝置上沒有任何應用程式存在，因此我們會安裝已取代的應用程式：App C。取代的應用程式是指取代鏈結中所有其他應用程式的應用程式。
	■：裝置上只有應用程式 A 和 C 存在。應用程式之間的關聯性是其中一個應用程式更新。 ■：沒有。	由於應用程式 C 已存在於裝置上，且這是應用程式更新案例，因此不會卸載應用程式 A。
	■：只有應用程式 A 存在於裝置上。應用程式之間的關聯性是其中一個應用程式更新。 ■：安裝 C。	只安裝 App C。應用程式 A 不會卸載，因為它是應用程式更新案例。C 的安裝程式不一定具有移除 A 的行為，其中「移除」表示 A 不再透過其偵測規則偵測 (通常是因為版本偵測)。
	■：裝置上只有 App C 存在。應用程式之間的關聯性是其中一個應用程式更新。 ■：沒有。	由於 App C 已取代的應用程式已存在於裝置上，而這是應用程式更新案例，因此不會採取任何動作。
	■：裝置上沒有任何應用程式存在。應用程式之間的關聯性是其中一個應用程式取代專案。 ■：安裝 C。	由於裝置上沒有任何應用程式存在，只要安裝取代的應用程式 App C 即可。
	■：應用程式 A 和 C 存在於裝置上。應用程式之間的關聯性是其中一個應用程式取代專案。 ■：卸載 A。	由於應用程式 C 存在於裝置上，而這是應用程式取代案例，因此只要卸載 App A 即可。

	■: 只有應用程式 A 存在於裝置上。應用程式之間的關聯性是其中一個應用程式取代專案。 ■: 卸載 A, 然後安裝 C。	由於這是應用程式取代案例, 因此會卸載應用程式 A, 並安裝 App C, 即已取代的應用程式。
	■: 裝置上只有 App C 存在。應用程式之間的關聯性是其中一個應用程式取代專案。 ■: 沒有。	由於已取代的應用程式 App C 存在於裝置上, 而且沒有其他已取代的應用程式存在, 因此不會採取任何動作。

取代限制

單一取代圖形中最多隻能有 10 個節點。節點包括已取代的應用程式、已取代的應用程式, 以及所有後續的相關應用程式。在下列取代圖表中, 總共有五個節點。因此, 在達到最大節點計數之前, 可以再建立五個節點。



其他取代限制：

- Azure 虛擬桌面多重會話僅支援與系統內容 (裝置型) 應用程式的取代關聯性。
- 取代公開預覽不支援 ESP (註冊狀態頁面)。ESP 會在新裝置註冊之後, 以及新使用者登入裝置時顯示布建進度。針對取代公開預覽版, 如果應用程式具有取代關聯性, 即使 ESP 原則中包含為選取的應用程式, 也不會在 ESP 期間強制執行。此外, 在 ESP 期間, 與取代關聯性相關的應用程式將不會傳送至用戶端裝置。不過, 應用程式會在 ESP 完成後傳送至裝置, 並遵守取代關聯性。
- 只有目標應用程式才會在 Microsoft 端點管理員 系統管理中心顯示安裝狀態。

後續步驟

- [針對 Win32 應用程式問題進行疑難排解](#)
- [使用 Microsoft Intune 監視應用程式資訊和指派](#)
- [Microsoft Intune 中的 Win32 應用程式管理](#)

Win32 應用程式問題疑難排解

2022/9/27 •

當您正在疑難排解 Microsoft Intune 中使用的 Win32 應用程式時，您可以使用一些方法。本文提供疑難排解的詳細資訊和資訊，可協助您解決 Win32 應用程式問題。如需詳細資訊，請參閱 [Win32 應用程式安裝疑難排解](#) 資源。

NOTE

此 app management 功能支援 Windows 應用程式的32位和64位作業系統架構。

IMPORTANT

當您部署 Win32 應用程式時，請考慮以獨佔方式使用 [Intune 管理擴充](#) 方法，尤其是當您具有多檔案 Win32 應用程式安裝程式時。如果您在 Autopilot 註冊期間混合安裝 Win32 應用程式和企業營運 (LOB) 應用程式，應用程式安裝可能會失敗。將 PowerShell 腳本或 Win32 應用程式指派給使用者或裝置時，會自動安裝 Intune 管理擴充。

針對根據使用者目標部署及指派 Win32 應用程式的案例，如果 Win32 應用程式需要裝置系統管理員許可權，或是裝置的標準使用者沒有任何其他許可權，則應用程式將無法安裝。

應用程式疑難排解詳細資料

您可以查看安裝問題，例如建立、修改、設定目標應用程式，以及將它傳遞至裝置。[Microsoft 端點管理員系統管理中心](#)提供「疑難排解 + 支援」窗格上的這些和其他詳細資料。如需詳細資訊，請參閱 [應用程式疑難排解的詳細資料](#)。

使用記錄檔疑難排解應用程式問題

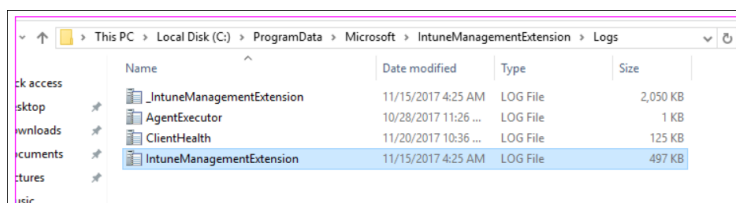
查看記錄的詳細資料可協助您判斷所看到問題的原因，並協助您加以解決。您可以選擇查看 [Intune 中顯示的記錄檔](#)，或 [透過 CMTrace 查看顯示的記錄](#)。

在 Intune 顯示記錄

當 Win32 應用程式發生安裝問題時，您可以在 [安裝詳細資料](#) 窗格中，針對 Intune 中的應用程式，選擇 [收集記錄] 選項。如需詳細資訊，請參閱 [Win32 應用程式安裝疑難排解](#)。

透過 CMTrace 顯示的記錄

用戶端電腦上的代理程式記錄通常是在 *C:\ProgramData\Microsoft\IntuneManagementExtension\Logs* 中。您可以使用 *CMTrace.exe* 來查看這些記錄檔。如需詳細資訊，請參閱 [CMTrace](#)。



Here is the path: c:\programdata\microsoft\intunemanagementextension\logs. You can download configMgr tools (cmtrace.exe) to view the log friendly and dynamically.

- a. IntuneManagementExtension.log is the main client log file, it contains all the agent check in, policy request, policy processing and reporting activities.
- b. AgentExecutor.log is the log file to track Powershell script execution details.
- c. ClientHealth.log is the log file to track sidcar agent client health activities

IMPORTANT

若要允許正確安裝和執行 LOB Win32 應用程式，反惡意程式碼設定應該會排除掃描下列目錄：

■ x64 ■：

C:\Program (x86) \ Microsoft Intune 管理 Extension\Content

C:\windows\IMECache

■ x86 ■：

C:\Program 檔 \ Microsoft Intune 管理 Extension\Content

C:\windows\IMECache

如需詳細資訊，請參閱[適用於目前支援 Windows 版本之企業電腦的病毒掃描建議](#)。

使用 PowerShell 偵測 Win32 應用程式檔版本

如果您在偵測 Win32 應用程式檔案版本時有困難，請考慮使用或修改下列 PowerShell 命令：

```
$FileVersion = [System.Diagnostics.FileVersionInfo]::GetVersionInfo("<path to binary file>").FileVersion
#The below line trims the spaces before and after the version name
$FileVersion = $FileVersion.Trim();
if ("<file version of successfully detected file>" -eq $FileVersion)
{
    #Write the version to STDOUT by default
    $FileVersion
    exit 0
}
else
{
    #Exit with non-zero failure code
    exit 1
}
```

在上述 PowerShell 命令中，以 Win32 應用程式檔案的路徑取代 `<path to binary file>` 字串。範例路徑類似下列所示：

```
C:\Program Files (x86)\Microsoft SQL Server Management Studio 18\Common7\IDE\ssms.exe
```

此外，請將字串取代 `<file version of successfully detected file>` 為您需要偵測的檔案版本。檔案版本字串範例類似下列所示：

```
2019.0150.18118.00 ((SSMS_Rel).190420-0019)
```

如果您需要取得 Win32 應用程式的版本資訊，可以使用下列 PowerShell 命令：

```
[System.Diagnostics.FileVersionInfo]::GetVersionInfo("<path to binary file>").FileVersion
```

在上述 PowerShell 命令中，以檔案路徑取代 `<path to binary file>` 。

其他應考慮的疑難排解區域

- 檢查目標，確定裝置上已安裝代理人。目標為群組的 Win32 應用程式或為群組的 PowerShell 腳本，將會建立安全性群組的代理安裝原則。
- 檢查作業系統版本：Windows 10 1607 和更新版本。
- 檢查 Windows 10 SKU。Windows 10 s 或 Windows 版本已啟用 S 模式，不支援 MSI 安裝。

如需疑難排解 Win32 應用程式的詳細資訊，請參閱 [win32 應用程式安裝疑難排解](#)。如需 ARM64 裝置上應用程式類型的相關資訊，請參閱 [ARM64 裝置上支援的應用程式類型](#)。

後續步驟

- [疑難排解應用程式安裝問題](#)

啟用 S 模式裝置上的 Win32 應用程式

2022/9/27 •

Windows 10 S 模式是只執行存放區應用程式的鎖定作業系統。依預設，Windows S 模式裝置不允許安裝和執行 Win32 應用程式。這些裝置包含單一 *Win 10S 基本原則*，此原則會鎖定 S 模式裝置，使其無法在其上執行任何 Win32 應用程式。不過，透過在 Intune 中建立及使用 S 模式補充原則，您可以在 Windows 10 S 模式受管理的裝置上安裝及執行 Win32 應用程式。使用 [Microsoft Defender Application Control \(WDAC\) PowerShell 工具](#)，您可以為 Windows S 模式建立一個或多個補充原則。您必須使用 [Device Guard 簽署服務 \(DGSS\)](#) 或 [SignTool.exe](#) 來簽署補充原則，然後透過 Intune 上傳及發佈原則。您也可以選擇使用組織的 codesigning 憑證簽署補充原則，但慣用的方式是使用 DGSS。在您從組織使用 codesigning 憑證的實例中，codesigning 憑證所連結的根憑證必須存在於裝置上。

在 Intune 中指派 S 模式補充原則，可讓裝置對裝置的現有 S 模式原則產生例外狀況，以允許上傳的對應已簽署應用程式目錄。原則會設定可在 S 模式裝置上使用之應用程式目錄的 [允許] 應用程式清單。

NOTE

在 S 模式裝置上的 Win32 應用程式只有在 Windows 10 11 月 2019 更新 (組建 18363) 或更新版本上支援。

允許 Win32 應用程式在 Windows 10 裝置上以 S 模式執行的步驟如下：

1. 在 Windows 10 的註冊程式中，透過 Intune 啟用 S 模式裝置。
2. 建立補充原則以允許 Win32 應用程式：
 - 您可以使用 [Microsoft Defender Application Control \(WDAC\)](#) 工具建立補充原則。原則中的基準原則識別碼必須符合在用戶端上進行硬式編碼 S 模式基準原則識別碼。此外，請確定原則版本高於先前的版本。
 - 您可以使用 DGSS 簽署補充原則。如需詳細資訊，請參閱 [使用 Device Guard 簽署的符號代碼完整性原則](#)。
 - 您可以建立 Windows 10 S 模式補充原則，將簽署的補充原則上傳至 Intune，(請參閱下列)。
3. 您可以透過 Intune 允許 Win32 應用程式目錄：
 - 您可以為每個應用程式建立目錄檔案 (1)，並使用 DGSS 或其他憑證基礎結構簽署這些檔案。
 - 您可以使用 [Microsoft Win32 內容準備工具](#)，將已簽署的編目打包成 *intunewin* 檔案。使用 [Microsoft Win32 內容準備工具](#) 建立目錄檔時，沒有命名限制。從指定的來源資料夾及安裝檔案產生 *intunewin* 檔案時，您可以使用 -a cmdline 選項，提供僅包含目錄檔案的個別資料夾。如需詳細資訊，請參閱 [win32 應用程式管理-準備用於上載的 win32 應用程式內容](#)。
 - Intune 會套用已簽署應用程式目錄，以在 S 模式裝置上使用 [Intune 管理副檔名](#) 安裝 Win32 應用程式。

NOTE

企業營運 (LOB) .appx 和 .appx Windows 10 S 模式上的東會透過商務用 Microsoft Store (MSFB) 簽署來支援。

應用程式的「」必須透過 Intune 管理擴充性來傳遞。

S 模式原則會在裝置層級強制執行。在裝置上會合併多個目標原則。合併的原則將會在裝置上強制執行。

若要建立 Windows 10 S 模式補充原則，請使用下列步驟：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 **應用程式 > S 模式補充原則 > 建立原則**。

3. 在新增 **原則** 檔案之前，您必須建立並簽署該檔案。如需詳細資訊，請參閱：

- [使用 PowerShell 工具建立 WDAC 原則，並將其轉換成二進位格式](#)
- [使用 Device Guard 簽署服務簽署服務 \(建議\)](#)

4. 在 [**基礎**] 頁面上，新增下列值：

I	II
原則檔	包含 WDAC 原則的檔案。
名稱	這個原則的名稱。
描述	選這個原則的描述。

5. 按 [**下一步：範圍標記**]。

在 [**範圍 標籤**] 頁面上，您可以選擇性地設定範圍標記，以決定誰可以查看 Intune 中的應用程式原則。如需有關範圍標籤的詳細資訊，請參閱 [使用角色型存取控制和範圍標籤來發佈它](#)。

6. 按 [**下一步：工作分派**]。

[**工作分派**] 頁面可讓您將原則指派給使用者和裝置。請務必注意，不論裝置是否由 Intune 所管理，都可以指派原則給裝置。

7. 按 [**下一步：複查 + 建立**] 以檢查您為設定檔輸入的值。

8. 完成後，按一下 [**建立**]，以在 Intune 中建立 S 模式補充原則。

建立原則之後，您會看到它會加入 Intune 中的 S 模式補充原則清單。指派原則之後，便會將原則部署至裝置。請注意，您必須將此應用程式部署至與補充原則相同的安全性群組。您可以開始設定目標，並指派應用程式至這些裝置。這可讓您的使用者在 S 模式裝置上安裝及執行應用程式。

移除 S 模式原則

目前，若要從裝置移除 S 模式補充原則，您必須指派及部署空白原則，以覆寫現有的 S 模式補充原則。

原則報告

在裝置層級強制執行的 S 模式補充原則，只具有裝置層級報告。裝置等級報告可用於成功和錯誤狀況。

顯示在 Intune 主控台其中的「S 模式」報告原則的報告值：

- **成功**：S 模式補充原則已生效。
- **未知**：不知道 S 模式補充原則的狀態。
- **TokenError**：S 模式補充原則是在結構上，但在授權權杖時發生錯誤。
- **NotAuthorizedByToken**：權杖不會授權此 S 模式補充原則。
- **PolicyNotFound**：未找到 S 模式補充原則。

後續步驟

- 如需詳細資訊，請參閱 [s 模式的 Win32 應用程式](#)。
- 如需將應用程式新增至 Intune 的詳細資訊，請參閱 [將應用程式新增至 Microsoft Intune](#)。
- 如需 win32 應用程式的詳細資訊，請參閱 [Intune win32 應用程式管理](#)。

在 Intune 中部署 Windows 更新套件

2022/9/27 •

若要將特定的 Windows 更新套件部署 (.msu file) 為由 Intune 管理的 Windows 10/11 裝置, 您可以使用 [Intune 的 win32 應用程式管理](#) 功能, 將 .msu 檔案部署為 Win32 應用程式。

下列步驟可協助您將 Windows 更新套件部署至 Intune。

步驟1: 將更新套件準備為 Win32 應用程式內容

1. 搜尋 [Microsoft update Catalog](#), 以下載 Windows 更新套件。
2. 使用 [Microsoft Win32 內容準備工具](#), 將 .msu 檔案轉換為 *intunewin* 格式。當您未在命令列中指定參數時, 此工具會引導您以逐步處理方式輸入必要的參數。如需 Microsoft Win32 內容準備工具的詳細資訊, 請參閱 [轉換 Win32 應用程式內容](#)。

步驟2: 建立 Win32 應用程式

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用 > > 程式][新增]。
3. 在 [選取應用程式類型] 窗格的 [其他 應用程式類型] 下, 選取 [Windows app (Win32)]。
4. 按一下 [選取], 找出 [新增應用程式] 窗格, 然後選取 [選取應用程式套件 檔案]。
5. 在 [應用程式套件 檔案] 窗格中, 選取 *intunewin* 檔案, 然後選取 [確定]。
6. 在 [應用程式資訊] 頁面上, 新增應用程式的詳細資料。
7. 在 [程式] 頁面上, 指定應用程式的下列安裝及移除命令:

安裝命令:

```
wusa.exe <full path of the .msu file> /quiet /norestart -Wait
```

例如, 如果 *windows 10.0-kb4532693-x64_e22f60a077a0ec5896266a18cc3daf26bfc29e16.msu* 檔案位於目前的資料夾中, 請在 **Install 命令** 中輸入下列命令:

```
wusa.exe .\windows10.0-kb4532693-x64_e22f60a077a0ec5896266a18cc3daf26bfc29e16.msu /quiet /norestart -Wait
```

卸載命令:

```
wusa.exe /uninstall /kb:<KB number> /quiet
```

下圖提供 **程式** 頁面的範例:

Edit application
Windows app (Win32)

App information Program Requirements Detection rules Review + save

Specify the commands to install and uninstall this app:

Install command * ⓘ

Uninstall command * ⓘ

Install behavior ⓘ System User

Device restart behavior ⓘ App install may force a device restart

Specify return codes to indicate post-installation behavior:

Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

[+ Add](#)

`/quiet` 使用參數，以安靜模式執行 *Wusa.exe*，而不需要使用者互動。`/norestart` 使用參數，避免 *Wusa.exe* 重新開機電腦。如需 *Wusa.exe* 的詳細資訊，請參閱 [Windows 中 Windows Update 獨立 Installer 的描述](#)。

使用此 `-wait` 選項，確定應用程式安裝會在 *Wusa.exe* 退出後傳回。

- 在 [需求] 頁面上，指定在安裝應用程式之前，裝置必須符合的 [需求](#)。

最低作業系統：選取套用更新所需的最低作業系統。

若要指定其他需求，例如組建編號和更新組建修訂 (UBR)，請選取 [新增]，以顯示 [新增需求規則] 窗格。

例如，若要在執行 Windows 10 的裝置上只安裝應用程式，版本1903，組建18362，UBR 小於329，請選取 **Registry** 做為 **要求類型**，然後指定下列規則：

- 索引 鍵路徑：
- 值名稱：CurrentBuildNumber
- 登錄機 碼需求：字串比較
- 運算子：等於
- 值：18362
- 與64位用戶端上的32位應用程式相關聯：否

Add a Requirement rule

Create a requirement.

Requirement type ⓘ Registry

Key path * ⓘ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows ...

Value name ⓘ CurrentBuildNumber

Registry key requirement * ⓘ String comparison

Operator * ⓘ Equals

Value * ⓘ 18362

Associated with a 32-bit app on 64-bit clients ⓘ Yes No

- 索引 鍵路徑: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
- 值名稱: UBR
- 登錄機 碼需求: 整數比較
- Operator: 小於
- 值: 329
- 與64位用戶端上的32位應用程式相關聯: 否

Add a Requirement rule

Create a requirement.

Requirement type ⓘ Registry

Key path * ⓘ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows ...

Value name ⓘ UBR

Registry key requirement * ⓘ Integer comparison

Operator * ⓘ Less than

Value * ⓘ 329

Associated with a 32-bit app on 64-bit clients ⓘ Yes No

9. 在 [偵測規則] 頁面上, 選取 [使用自訂偵測腳本 做為 規則格式]。

範例:

Windows app (Win32)

Windows app (Win32)

App informationProgramRequirementsDetection rulesReview + save

Configure app specific rules used to detect the presence of the app.

Rules format *

Use a custom detection script

Script file

Select a file

Run script as 32-bit process on 64-bit clients

YesNo

Enforce script signature check and run script silently

YesNo

(DetectKB.ps1) 範例腳本 檔案：

```
$result = systeminfo.exe | findstr KB<KB number>

if ($result)
{
    Write-Output "Found KB<KB number>"
    exit 0
}
else
{
    exit 1
}
```

- 指定應用程式的 [指派](#)。
- 請複查您的設定，然後選取 [建立]，將應用程式新增至 Intune。

步驟3: 部署應用程式

[指派應用程式](#) 至群組。

後續步驟

- 如需將應用程式新增至 Intune 的詳細資訊，請參閱[將應用程式新增至 Microsoft Intune](#)。
- 如需 win32 應用程式的詳細資訊，請參閱[Intune win32 應用程式管理](#)。

新增並指派受控裝置的Windows 10 公司入口網站應用程式Intune

2022/9/27 •

若要管理裝置並安裝應用程式，您的使用者可以選擇性地使用公司入口網站應用程式。您可以直接從 Intune 指派Windows 10 公司入口網站應用程式。

必要條件

您可以選擇使用下列步驟來安裝 **公司入口網站 (Offline)** 應用程式。將公司入口網站應用程式指派給 Autopilot 群組時，將會安裝在裝置內容中，並且會在使用者登入之前安裝在裝置上。離線應用程式會使用Intune更新，而線上應用程式則由市集更新。當您需要安裝和維護特定應用程式版本時，請使用離線應用程式。

針對Windows 10 Autopilot 布建的裝置，建議您將商務用 Microsoft Store帳戶與Intune建立關聯。如需詳細資訊，請參閱[如何使用 Microsoft Intune 從商務用 Microsoft Store管理大量購買的應用程式](#)。

設定市集設定以顯示離線應用程式

1. 使用您的系統管理員帳戶登入[商務用 Microsoft Store](#)。
2. 選取接近視窗頂端的 [管理] 索引標籤。
3. 在左窗格中，選取 [設定]。
4. 在 [購物體驗] 底下，將 [顯示離線應用程式] 設定為 [開啟]。
離線授權應用程式隨即顯示。

從市集取得離線公司入口網站應用程式

1. 搜尋並選取 **公司入口網站** 應用程式。
2. 將 [授權類型] 設定為 [離線]。
3. 選取 [取得要取得的應用程式]，並將離線公司入口網站應用程式新增至您的庫存。若要讓應用程式列在 Intune中，您必須等候同步排程完成，或從 Microsoft 端點管理員 系統管理中心進行手動同步處理。

使用 Intune 手動同步處理公司入口網站應用程式

1. 使用您的系統管理員帳戶登入[Microsoft 端點管理員 系統管理中心](#) 。
2. 選取 [租使用者系統管理 > 連接器和權杖 > 商務用 Microsoft Store]。
3. 按一下 [啟用]。
4. 如果您尚未這麼做，請按一下連結以註冊商務用 Microsoft Store，並如先前所述將您的帳戶建立關聯。
5. 從 [語言] 下拉式清單中，選擇入口網站中顯示商務用 Microsoft Store應用程式的語言。不論顯示的語言為何，它們都會在可用時以使用者的語言安裝。
6. 按一下 [同步]，將您從 Microsoft Store 購買的應用程式放入Intune。

指派公司入口網站應用程式

1. 使用您的系統管理員帳戶登入[Microsoft 端點管理員 系統管理中心](#) 。
2. 選取 [應用程式 > 視窗]。
3. 從 Windows 應用程式清單中，選 **公司入口網站 (離線)**。
4. 若 **要將**公司入口網站應用程式指派為所選裝置群組的必要應用程式，請選 > 取 [指派] 旁的 [屬性 編輯 () >

[必要)] 底 下的 [新增群組 (], 然後選取要指派應用程式的裝置群組。

5. 由於這是 離線 應用程式, 請務必在選取 [檢閱 + 儲存] 之前, 將 [授權類型] 變更為 [裝置授權]。若要設定 [授權類型], 請按一下您在 [授權類型] 資料行) 底下新增 (群組資料列的 [使用者]。
6. 選 取 [裝置授權 > 確定 > 檢閱 + 儲存]。

後續步驟

- 若要深入瞭解如何指派應用程式, 請 [參閱將應用程式指派給群組](#)。

使用 Microsoft Intune 新增 Windows 10 公司入口網站應用程式

2022/9/27 •

若要管理裝置並安裝應用程式，您的使用者可以從 Microsoft Store 自行安裝公司入口網站應用程式。不過，如果您的業務需要要求您將公司入口網站應用程式指派給他們，您可以直接從 Intune 指派 Windows 10 公司入口網站應用程式。即使您尚未將 Intune 與商務用 Microsoft Store 整合，您也可以這麼做。

IMPORTANT

如果您下載公司入口網站應用程式，本文所述的選項會要求您在每次發行應用程式更新時指派手動更新。若要為 Windows 10 Autopilot 布建的裝置部署公司入口網站應用程式，請參閱[新增 Windows 10 公司入口網站應用程式 Autopilot 裝置](#)。

NOTE

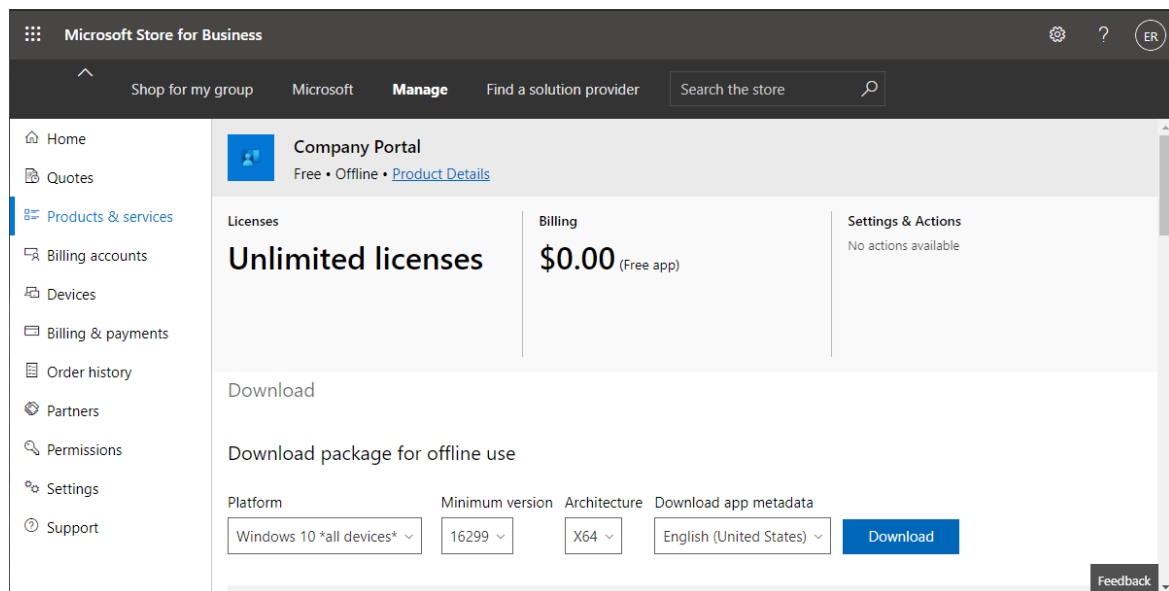
公司入口網站支援 Configuration Manager 應用程式。這項功能可讓終端使用者在共同管理的客戶公司入口網站中看到 Configuration Manager 和 Intune 部署的應用程式。這個新版本的公司入口網站會為所有共同管理的客戶顯示 Configuration Manager 部署的應用程式。這項支援可協助系統管理員合併其不同的使用者入口網站體驗。如需詳細資訊，請參閱[在共同管理的裝置上使用公司入口網站應用程式](#)。

設定設定以顯示離線應用程式

1. 使用您的系統管理員帳戶登入[商務用 Microsoft Store](#)。請確定您使用您用來登入 Intune 的相同租使用者帳戶來登入商務用 Microsoft Store。您的商務用 Microsoft Store 帳戶必須與 Intune 相關聯。如需詳細資訊，請參閱[將商務用 Microsoft Store 帳戶與 Intune 建立關聯](#)。
2. 選取接近視窗頂端的 [管理] 索引標籤。
3. 在左窗格中，選取 [設定]。
4. 選取 [商店] 索引標籤。然後，在 [購物體驗] 下，將 [顯示離線應用程式] 設定為 [開啟]。

下載離線公司入口網站應用程式

1. 搜尋並選取 公司入口網站 應用程式。
2. 將 [授權類型] 設定為 [離線]。離線應用程式是由 Intune 所管理，而線上應用程式則由市集管理。當您需要安裝和維護特定應用程式版本時，請使用離線應用程式。
3. 選取 [取得要取得的應用程式]，並將離線公司入口網站應用程式新增至您的庫存。如果您已經有離線應用程式，您可以選取 [管理] 選項。
4. 針對 [平臺]，選取 [Windows 10 所有裝置]，然後選取適當的 [最低版本]、[架構] 和 [下載應用程式中繼資料] 值。
5. 選取 [下載] 將檔案儲存至本機電腦。



6. 選取[下載]，以下載 [必要架構] 下的所有套件。

此動作必須針對 x86、x64 和 ARM 架構完成：

選取 1507 做為最低作業系統版本時，有 9 個必要架構套件，選取 1511 時有 12 個套件，選取 1607 時有 15 個套件。

7. 在入口網站Microsoft Intune中，將公司入口網站應用程式上傳為新的應用程式。您可以在 [選取應用程式類型] 窗格中選取 [企業營運應用程式] 作為 [應用程式類型] 來新增應用程式。然後選取應用程式套件檔案 (副檔名 .AppxBundle)。
8. 在 [選取相依性應用程式檔案] 下，使用 shift-click 選取您在步驟 7 中下載的所有相依性，並確認 [新增] 資料行會針對您需要的架構顯示 [是]。

NOTE

如果未新增相依性，應用程式可能不會安裝在指定的裝置類型上。

9. 按一下 [確定]，輸入任何所需的 應用程式資訊，然後按一下 [新增]。
10. 將公司入口網站應用程式指派為您選取的使用者或裝置群組集合的必要應用程式。

如需Intune如何處理通用應用程式相依性的詳細資訊，請參閱[透過 Microsoft Intune MDM 部署具有相依性的 appxbundle](#)。

常見問題集

NOTE

Microsoft Intune將於 2022 年 10 月 21 日終止對執行 Windows 8.1 之裝置的支援。Intune將不再支援側載Windows 8.1。

如果使用者已從市集安裝較舊的應用程式，如何?更新使用者裝置上的公司入口網站應用程式？

如果您的使用者已從 Microsoft Store 安裝Windows 8.1 公司入口網站應用程式，其應用程式應該會自動更新為最新版本，而不需要您或您的使用者採取任何動作。如果未進行更新，請要求您的使用者確認他們已在其裝置上啟用市集應用程式的自動更新。

如何?將我的側載Windows 8.1 公司入口網站應用程式升級至Windows 10 公司入口網站應用程式？

我們建議的移轉路徑是藉由將指派動作設定為 [卸載] 來刪除Windows 8.1 公司入口網站應用程式的指派。選取此設定之後，您可以使用先前討論過的任何選項來指派Windows 10 公司入口網站應用程式。

如果您需要側載應用程式，且您指派了Windows 8.1 公司入口網站，但未使用 Symantec 憑證簽署它，請完成本文前幾節中的步驟來完成升級。

如果您需要側載應用程式，並使用 Symantec 程式碼簽署憑證簽署並指派Windows 8.1 公司入口網站應用程式，請遵循下一節中的步驟。

如何?將已簽署並側載的Windows 8.1 公司入口網站應用程式升級至Windows 10 公司入口網站應用程式?

我們建議的移轉路徑是藉由將指派動作設定為 [卸載] 來刪除Windows 8.1 公司入口網站應用程式的現有指派。選取此設定之後，您可以正常指派Windows 10 公司入口網站應用程式。

否則，必須適當地更新和簽署Windows 10 公司入口網站應用程式，以確保遵守升級路徑。

如果您以這種方式簽署並指派Windows 10 公司入口網站應用程式，則在市場中提供每個新的應用程式更新時，您必須針對每個新的應用程式更新重複此程式。更新市場時，不會自動更新應用程式。

以下是以這種方式簽署和指派應用程式的方式：

1. 下載[Microsoft Intune Windows 10 公司入口網站應用程式簽署腳本](#)。
此腳本需要將 Windows SDK for Windows 10安裝在主機電腦上。[下載適用於 Windows 10 的 Windows SDK](#)。
2. 如先前所述，從商務用 Microsoft Store下載Windows 10 公司入口網站應用程式。
3. 若要簽署Windows 10 公司入口網站應用程式，請使用腳本標頭中詳述的輸入參數來執行腳本，如下表所示。
相依性不需要傳遞至腳本。只有當應用程式上傳至 Intune 管理員 主控台時，才需要它們。

“	“
InputWin10AppxBundle	來源 appxbundle 檔案的路徑。
OutputWin10AppxBundle	已簽署 appxbundle 檔案的輸出路徑。
Win81Appx	Windows 8.1 公司入口網站 (的路徑。APPX) 檔案。
PfxFilePath	Symantec Enterprise 行動程式碼簽署憑證的路徑 (。PFX) 檔案。
PfxPassword	Symantec Enterprise Mobile Code 簽署憑證的密碼。
PublisherId	企業的發行者識別碼。如果不存在，則會使用 Symantec Enterprise Mobile Code 簽署憑證的 [主體] 欄位。
SdkPath	適用於 Windows 10 之 Windows SDK 根資料夾的路徑。此引數是選擇性的，預設為 <code>\${env:ProgramFiles (x86)}\Windows Kits\10</code> 。

當腳本完成執行時，它會輸出Windows 10 公司入口網站應用程式的已簽署版本。然後，您可以透過 Intune 將已簽署的應用程式版本指派為企業營運 (LOB) 應用程式，這會將目前指派的版本升級至這個新的應用程式。

後續步驟

- [將應用程式指派給群組](#)

新增 macOS 公司入口網站應用程式

2022/9/27 •

若要在具有使用者關聯性的 macOS 裝置上管理裝置、安裝選用的應用程式，以及存取受條件存取保護的資源，使用者必須安裝並登入公司入口網站應用程式。您可以為使用者提供指示，以安裝 macOS 的公司入口網站，或將其安裝在已直接從 Intune 註冊的裝置上。

您可以使用下列任一選項來安裝 macOS 應用程式的公司入口網站：

- [指示使用者下載及安裝公司入口網站](#)
- [以 macOS LOB 應用程式的公司入口網站形式安裝 macOS](#)
- [使用 macOS 命令介面腳本安裝 macOS 的公司入口網站](#)

若要協助您在安裝應用程式時，將其保持在最新狀態，則公司入口網站應用程式隨附 Microsoft AutoUpdate (MAU)。

NOTE

[！注意] 只有在使用直接註冊或自動裝置註冊註冊的 Intune 裝置上，才能自動安裝公司入口網站應用程式。若為個人裝置或手動註冊，必須下載並安裝公司入口網站應用程式，才能啟動註冊。請參閱[指示使用者下載及安裝公司入口網站](#)。

指示使用者下載及安裝公司入口網站

您可以指示使用者為 macOS 下載、安裝和登入公司入口網站。如需下載、安裝和登入公司入口網站的相關指示，請參閱[使用公司入口網站 app 註冊 macOS 裝置](#)。

NOTE

當您下載 macOS 裝置版本 2.18.2107 及更新版本的 Intune 公司入口網站時，它會安裝在 Apple 矽 mac 上以本機方式執行的新通用版應用程式。相同的應用程式會在 Intel Mac 機上安裝 x64 版本的應用程式。

以 macOS LOB 應用程式的公司入口網站形式安裝 macOS

您可以使用 [macOS LOB app](#) 功能下載及安裝 macOS 的公司入口網站。下載的版本是永遠安裝的版本，而且可能需要定期更新，以確保使用者在初次註冊時取得最佳的體驗。

1. 下載 macOS <https://go.microsoft.com/fwlink/?linkid=853070> 的公司入口網站。
2. 依照指示在 [MACOS LOB 應用程式](#) 中建立 macOS lob 應用程式。

NOTE

安裝之後，macOS 應用程式的公司入口網站會使用 Microsoft AutoUpdate (MAU) 自動更新。

使用 macOS 命令介面腳本安裝 macOS 的公司入口網站

您可以使用 [macOS 命令介面腳本](#) 功能下載及安裝 macOS 的公司入口網站。此選項一定會為 macOS 安裝目前版本的公司入口網站，但不會提供應用程式安裝報告，當您使用 [macOS LOB 應用程式](#) 部署應用程式時，您可能需要使用這些報告。

1. 下載範例腳本，以從[Intune 命令介面腳本範例-公司入口網站](#)安裝 macOS 的公司入口網站。
2. 依照指示，使用 [MacOS 命令介面腳本](#)部署 macOS 命令介面腳本。
 - 在 [系統內容] 中，將 run 腳本 設定為 無 (執行)。
 - 設定 [腳本失敗時的重試次數上限]。

NOTE

腳本會在執行時要求網際網路存取，以下載 macOS 的目前公司入口網站版本。

在使用具有新式驗證的設定助理時，登入 macOS 的公司入口網站

若為執行10.15 和更新版本的 macOS 裝置，當您建立自動裝置註冊設定檔時，您現在可以選擇新的驗證方法：**具有新式驗證的設定助理**。使用者必須在設定助理畫面期間使用 Azure AD 認證進行驗證。這需要在公司入口網站應用程式中進行額外的 Azure AD 登入註冊，以存取由條件式存取和 Intune 所保護的公司資源，以評估裝置的合規性。您可以使用下列三種方式來安裝公司入口網站，以進行「新式驗證」的設定助理使用。

使用以上所述的方法之一，將 macOS 公司入口網站部署至使用「設定助理」(新式驗證)登錄的裝置，讓使用者能夠驗證並完成 Azure AD 註冊。

使用者必須登入公司入口網站，才可完成 Azure AD 驗證，並取得以條件式存取權保護的資源。當使用者完成註冊並進入 macOS 裝置的首頁畫面時，就會建立使用者相關性。如果承租人已開啟這些裝置或使用者的多重要素驗證，則系統會要求使用者在安裝助理期間進行註冊時，完成多重要素驗證。不需要多重要素驗證，但如有需要，可在條件式存取中使用此驗證方法。

如需使用 macOS 新式驗證設定設定助理的詳細資訊，請參閱 [Create An Apple 註冊設定檔](#)。

後續步驟

- 若要深入瞭解指派應用程式，請參閱 [將應用程式指派給群組](#)。
- 若要深入瞭解如何設定自動裝置註冊，請參閱 [Device 登記計畫-登記 macOS](#)。
- 若要深入瞭解如何在 macOS 上設定 Microsoft AutoUpdate 設定，請參閱 [Mac 更新](#)。

將 Windows 10/11 的 Microsoft Edge 新增至 Microsoft Intune

2022/9/27 •

您必須先將應用程式新增至Intune，才能部署、設定、監視或保護應用程式。其中一個可用的 [應用程式類型](#) 是 Microsoft Edge 77 版和更新版本。藉由在 Intune 中選取此應用程式類型，您可以將Microsoft Edge 77 版和更新版本指派及安裝到您管理執行Windows 10的裝置。

IMPORTANT

此應用程式類型為Windows 10提供穩定、Beta 和開發通道。部署僅使用英文 (EN)，不過終端使用者可以在瀏覽器的 [■ > Languages] 下變更顯示語言。Microsoft Edge是在系統內容中安裝的 Win32 應用程式，以及 x86 OS 上的 x86 應用程式和 x64 OS) 上 x64 應用程式 (架構。Intune會偵測任何預先存在的Microsoft Edge安裝。如果安裝在使用者內容中，系統安裝將會覆寫它。如果安裝在系統內容中，則會回報安裝成功。此外，Microsoft Edge的自動更新預設為 ■。

NOTE

Microsoft Edge 77 版和更新版本 也適用於 macOS。

您無法對加入工作區的電腦使用 Microsoft Edge 的內建應用程式部署。內建的應用程式部署需要 Intune 管理擴充功能，且僅限加入 AAD 的裝置。您仍然可以使用上傳至 ■ 的 .msi 部署Microsoft Edge 77 版和更新版本，請參閱 [將Windows企業營運應用程式新增至Microsoft Intune](#)。

必要條件

- Windows 10 1709 版或更新版本。
- 使用者內容中所有通道的任何預先安裝Microsoft Edge 版本 77 和 更新版本，都會以系統內容中安裝的 Edge 覆寫。

在 Intune 中設定應用程式

您可以使用下列步驟，將Microsoft Edge 77 版和更新版本新增至 Intune：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 >][所有應用程式 >][新增]。
3. 在 Microsoft Edge 77 版和更新版本 下的 [應用程式類型] 清單中，選取 [Windows 10]。

設定應用程式資訊

在此步驟中，您會提供此應用程式部署的相關資訊。此資訊可協助您在Intune中識別應用程式，並協助使用者在公司入口網站中尋找應用程式。

1. 按一下 [應用程式資訊] 以顯示 [應用程式資訊] 窗格。
2. 在 [應用程式資訊] 窗格中，您會提供此應用程式部署的相關資訊。此資訊可協助您在Intune中識別應用程式，並協助使用者在公司入口網站中尋找應用程式。
 - **名稱**：輸入將在公司入口網站中顯示的應用程式名稱。請確定所有名稱都是唯一的。如果相同的應用程式名稱存在兩次，公司入口網站中只會向使用者顯示其中一個應用程式。
 - **描述**：輸入應用程式的描述。例如，您可以在描述中列出目標使用者。

- **Publisher** : Microsoft 會顯示為發行者。
- **類別** : 選擇性地選取一或多個內建應用程式類別或您所建立的類別。此設定可讓使用者在流覽公司入口網站時更容易找到應用程式。
- **在公司入口網站中將此顯示為精選應用程式** : 選取此選項可在使用者流覽應用程式時, 在公司入口網站的主頁面上以醒目提示的方式顯示應用程式。
- **資訊 URL** : 選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
- **隱私權 URL** : 選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
- **開發人員** : Microsoft 會顯示為開發人員。
- **擁有者** : Microsoft 會顯示為擁有者。
- **附注** : 選擇性地輸入您想要與此應用程式相關聯的任何附注。

3. 選取 [確定]。

設定應用程式設定

在此步驟中, 設定應用程式的安裝選項。

1. 在 [新增應用程式] 窗格中, 選取 [應用程式設定]。
2. 在 [應用程式設定] 窗格中, 從 [通道] 清單中選取 [穩定]、[Beta] 或 [開發], 以判斷您將從哪個 Edge 通道部署應用程式。如需詳細資訊, [請參閱Microsoft Edge發行排程](#)。
 - **穩定** 通道是在Enterprise環境中廣泛部署的建議通道。它會每四周更新一次, 每個版本都會納入 Beta 通道的改善。
 - **Beta** 通道是最穩定Microsoft Edge預覽體驗, 也是組織內完整試驗的最佳選擇。每四周進行一次重大更新, 每個版本都會納入開發人員通道的學習和改善。
 - **開發** 人員通道已準備好在 Windows、Windows Server 和 macOS 上提供企業意見反應。它會每週更新一次, 並包含最新的改善和修正程式。

NOTE

當使用者流覽公司入口網站時, Microsoft Edge瀏覽器標誌會與應用程式一起顯示。

3. 選取 [確定]。

選取選擇性 (範圍標籤)

您可以使用範圍標籤來判斷誰可以在Intune中看到用戶端應用程式資訊。如需範圍標籤的完整詳細資料, 請參閱[針對分散式 IT 使用角色型存取控制和範圍標籤](#)。

1. 選取 [範圍 (標籤) > 新增]。
2. 使用 [選取] 方塊來搜尋範圍標籤。
3. 選取您要指派給此應用程式的範圍標籤旁的核取方塊。
4. 按一下 [選取 >] [確定]。

新增應用程式

當您完成設定應用程式時, 請從 [應用程式] 窗格中選取 [新增]。

您所建立的應用程式會顯示在應用程式清單中, 您可以將它指派給您選取的群組。

NOTE

目前，如果您取消指派Microsoft Edge的部署，它會保留在裝置上。

卸載應用程式

當您需要從使用者的裝置卸載Microsoft Edge時，請使用下列步驟。

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 >][所有應用程式 > Microsoft Edge 應用程式 > [指派 >][新增群組]。
3. 在 [新增群組] 窗格中，選取 [卸載]。

NOTE

如果Intune先前已透過  或使用相同部署的必要  應用程式安裝到裝置上，則會從選取群組中的裝置卸載應用程式。

4. 選取 [包含的群組] 以選取受此應用程式指派影響的使用者群組。
5. 選取您要套用卸載指派的群組。
6. 按一下 [選取群組] 窗格上的 [選取]。
7. 按一下 [指派] 窗格上的 [確定] 以設定指派。
8. 如果您想要排除任何使用者群組不受此應用程式指派影響，請選取 [排除群組]。
9. 如果您已選擇排除任何群組，請在 [選取群組] 中選取 [選取]。
10. 在 [新增群組] 窗格中選取 [確定]。
11. 在 [應用程式指派] 窗格中選取 [儲存]。

IMPORTANT

若要成功卸載應用程式，請務必先移除要安裝的成員或群組指派，再將它們指派給卸載。如果將群組指派給安裝應用程式和卸載應用程式，則應用程式會保留且不會移除。

疑難排解

Microsoft Edge 77 版和更新版本的 Windows 10：

Intune使用Intune管理延伸模組，將Microsoft Edge安裝程式下載並部署到指派的Windows 10裝置，然後將部署設定傳達給Microsoft Edge安裝程式，以下載並安裝Microsoft Edge 直接從CDN瀏覽器。參考[Intune管理延伸模組的必要條件](#)，以及存取 Azure 更新服務和CDN中概述的最佳做法，以確保您的網路設定允許Windows 10裝置存取這些位置。此外，若要允許從CDN存取安裝檔案以安裝瀏覽器，您必須允許存取Windows Update端點。如需詳細資訊，請參閱[管理Windows 10 版本 1809的連線端點 – Windows Update](#)和[Microsoft Intune 的網路端點](#)。

後續步驟

- [將應用程式指派給群組](#)

使用 Microsoft Intune 將 Microsoft Edge 新增至 macOS 裝置

2022/9/27 •

您必須先將應用程式新增至Intune，才能部署、設定、監視或保護應用程式。其中一個可用的 [應用程式類型](#) 是 Microsoft Edge 77 版和更新版本。藉由在 Intune 中選取此應用程式類型，您可以將Microsoft Edge 77 版和更新版本指派及安裝到您管理執行 macOS 的裝置。此應用程式類型可讓您輕鬆地將Microsoft Edge指派給 macOS 裝置，而不需要您使用 macOS 應用程式包裝工具。為了協助讓應用程式更安全且最新，應用程式隨附 Microsoft AutoUpdate (MAU)。

IMPORTANT

此應用程式類型提供 macOS 的開發人員和 Beta 通道。部署僅使用英文 (EN)，不過終端使用者可以在瀏覽器的 [■ > Languages] 下變更顯示語言。

NOTE

Microsoft Edge 77 版和更新版本 也適用於Windows 10。

必要條件

- macOS 裝置必須先執行 macOS 10.14 或更新版本，才能安裝Microsoft Edge。

將Microsoft Edge新增至 Intune

您可以使用下列步驟，將Microsoft Edge 77 版和更新版本新增至 Intune：

- 登入 [Microsoft 端點管理員系統管理中心](#)。
- 選取 [應用程式 >][所有應用程式 >][新增]。
- 在 Microsoft Edge 77 版和更新版本 下的 [應用程式類型] 清單中，選取 [macOS]。

設定應用程式資訊

在此步驟中，您會提供此應用程式部署的相關資訊。此資訊可協助您在Intune中識別應用程式，並協助使用者在公司入口網站中尋找應用程式。

- 按一下 [應用程式資訊] 以顯示 [應用程式資訊] 窗格。
- 在 [應用程式資訊] 窗格中，您會提供此應用程式部署的相關資訊。此資訊可協助您在Intune中識別應用程式，並協助使用者在公司入口網站中尋找應用程式。
 - 名稱**：輸入將在公司入口網站中顯示的應用程式名稱。請確定所有名稱都是唯一的。如果相同的應用程式名稱存在兩次，公司入口網站中只會向使用者顯示其中一個應用程式。
 - 描述**：輸入應用程式的描述。例如，您可以在描述中列出目標使用者。
 - Publisher**：Microsoft 會顯示為發行者。
 - 類別**：選擇性地選取一或多個內建應用程式類別或您所建立的類別。此設定可讓使用者在流覽公司入口網站時更容易找到應用程式。
 - 在公司入口網站中將此顯示為精選應用程式**：選取此選項可在使用者流覽應用程式時，在公司入口網站的主頁面上以醒目提示的方式顯示應用程式。

- **資訊 URL** :選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
- **隱私權 URL** :選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
- **開發人員** :Microsoft 會顯示為開發人員。
- **擁有者** :Microsoft 會顯示為擁有者。
- **附注** :選擇性地輸入您想要與此應用程式相關聯的任何附注。

3. 選取 [確定]。

設定 Microsoft Edge 設定

在此步驟中，設定應用程式的安裝選項。

1. 在 [新增應用程式] 窗格中，選取 [應用程式設定]。
2. 在 [應用程式設定] 窗格中，從 [通道] 清單中選取 [穩定]、[Beta] 或 [開發]，以判斷您將從哪個 Edge 通道部署應用程式。如需詳細資訊，[請參閱Microsoft Edge發行排程](#)。
 - **穩定** 通道是在Enterprise環境中廣泛部署的建議通道。它會每四周更新一次，每個版本都會納入 Beta 通道的改善。
 - **Beta** 通道是最穩定Microsoft Edge預覽體驗，也是組織內完整試驗的最佳選擇。每四周進行一次重大更新，每個版本都會納入開發人員通道的學習和改善。
 - **開發** 人員通道已準備好在 Windows、Windows Server 和 macOS 上提供企業意見反應。它會每週更新一次，並包含最新的改善和修正程式。

NOTE

當使用者流覽公司入口網站時，Microsoft Edge瀏覽器標誌會與應用程式一起顯示。

3. 選取 [確定]。

選取選擇性 (範圍標籤)

您可以使用範圍標籤來判斷誰可以在Intune中看到用戶端應用程式資訊。如需範圍標籤的完整詳細資料，請參閱[針對分散式 IT 使用角色型存取控制和範圍標籤](#)。

1. 選取 [範圍 (標籤) > 新增]。
2. 使用 [選取] 方塊來搜尋範圍標籤。
3. 選取您要指派給此應用程式的範圍標籤旁的核取方塊。
4. 按一下 [選取 >][確定]。

新增應用程式

完成設定後，請從 [應用程式] 窗格中選取 [新增]。

您所建立的應用程式會顯示在應用程式清單中，您可以將它指派給您選取的群組。

後續步驟

- 若要瞭解如何在 macOS 裝置上設定Microsoft Edge，請參閱[設定 macOS 裝置上的Microsoft Edge](#)。
- 若要瞭解如何從使用者群組中包含和排除應用程式指派，請參閱[包含和排除應用程式指派](#)。
- [將應用程式指派給群組](#)

使用 Microsoft Intune 將適用於端點的 Microsoft Defender新增至 macOS 裝置

2022/9/27 •

您必須先將應用程式新增至Intune，才能部署、設定、監視或保護應用程式。其中一個可用的[應用程式類型](#)是適用於端點的 Microsoft Defender。藉由在Intune中選取此應用程式類型，您可以將適用於端點的 Microsoft Defender指派並安裝到您管理執行 macOS 的裝置。此應用程式類型可讓您輕鬆地將適用於端點的 Microsoft Defender指派給 macOS 裝置，而不需要您使用 macOS 應用程式包裝工具。為了協助讓應用程式更安全且最新，應用程式隨附 Microsoft AutoUpdate (MAU)。

必要條件

- macOS 裝置必須執行 macOS 10.13 或更新版本。
- macOS 裝置必須至少有 650 MB 的磁碟空間。
- 在 Intune 中部署核心延伸模組。如需詳細資訊，請參閱在 [Intune 中新增 macOS 核心延伸模組](#)。

IMPORTANT

只有在安裝適用於端點的 Microsoft Defender 應用程式之前，核心延伸模組存在於裝置上時，才能自動核准。否則，使用者會在 Mac 上看到「系統擴充功能已封鎖」訊息，而且必須移至 [設定] 或 [設定 > [安全性 & [隱私權]，然後選取 [隱私權]，以核准擴充功能。如需詳細資訊，請參閱[針對 Mac 版 適用於端點的 Microsoft Defender](#)中的核心延伸模組問題進行疑難排解。

將適用於端點的 Microsoft Defender新增至 Intune

您可以使用下列步驟，將適用於端點的 Microsoft Defender新增至Intune：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 >][所有應用程式 >][新增]。
3. 在 [應用程式類型] 清單的 [適用於端點的 Microsoft Defender] 底下，選取 [macOS]。

設定應用程式資訊

在此步驟中，您會提供此應用程式部署的相關資訊。此資訊可協助您在Intune中識別應用程式，並協助使用者在公司入口網站中尋找應用程式。

1. 按一下 [應用程式資訊] 以顯示 [應用程式資訊] 窗格。
2. 在 [應用程式資訊] 窗格中，您會提供此應用程式部署的相關資訊。此資訊可協助您在Intune中識別應用程式，並協助使用者在公司入口網站中尋找應用程式。
 - **名稱**：輸入將在公司入口網站中顯示的應用程式名稱。請確定所有名稱都是唯一的。如果相同的應用程式名稱存在兩次，公司入口網站中只會向使用者顯示其中一個應用程式。
 - **描述**：輸入應用程式的描述。例如，您可以在描述中列出目標使用者。
 - **Publisher**：Microsoft 會顯示為發行者。
 - **類別**：選擇性地選取一或多個內建應用程式類別或您所建立的類別。此設定可讓使用者在流覽公司入口網站時更容易找到應用程式。
 - **在公司入口網站中將此顯示為精選應用程式**：選取此選項可在使用者流覽應用程式時，在公司入口網站的主頁面上以醒目提示的方式顯示應用程式。
 - **資訊 URL**：選擇性地輸入包含此應用程式相關資訊的網站 URL。URL 會顯示給公司入口網站中的使用

者。

- **隱私權 URL**：選擇性地輸入包含此應用程式隱私權資訊的網站 URL。URL 會顯示給公司入口網站中的使用者。
- **開發人員**：Microsoft 會顯示為開發人員。
- **擁有者**：Microsoft 會顯示為擁有者。
- **附注**：選擇性地輸入您想要與此應用程式相關聯的任何附注。

3. 選取 [確定]。

選取選擇性 (範圍標籤)

您可以使用範圍標籤來判斷誰可以在Intune中看到用戶端應用程式資訊。如需範圍標籤的完整詳細資料，請參閱[針對分散式 IT 使用角色型存取控制和範圍標籤](#)。

1. 選取 [範圍 (標籤) > 新增]。
2. 使用 [選取] 方塊來搜尋範圍標籤。
3. 選取您要指派給此應用程式的範圍標籤旁的核取方塊。
4. 按一下 [選取 >][確定]。

新增應用程式

完成設定後，請從 [應用程式] 窗格中選取 [新增]。

您所建立的應用程式會顯示在應用程式清單中，您可以將它指派給您選取的群組。

NOTE

目前，Apple 無法讓Intune在 macOS 裝置上卸載適用於端點的 Microsoft Defender。

後續步驟

- 若要瞭解 macOS 上適用於端點的 Microsoft Defender的Intune型部署，請參閱[macOS 上適用於端點的 Microsoft Defender的Intune型部署](#)
- 若要瞭解如何在 Intune 中套用端點安全性的防毒軟體原則，請參閱[Intune 中端點安全性的防毒軟體原則](#)
- 若要瞭解如何從使用者群組中包含和排除應用程式指派，請參閱[包含和排除應用程式指派](#)。
- 若要瞭解如何在Intune中將應用程式指派給群組，請參閱[將應用程式指派給群組](#)。

在 Windows 10/11 裝置上使用 PowerShell 腳本 Intune

2022/9/27 •

使用 Microsoft Intune 管理延伸模組，在 Intune 中上傳 PowerShell 腳本。然後，在 Windows 10 裝置上執行這些腳本。管理延伸模組可增強 MDM (Windows 裝置管理，並讓您更輕鬆地移至新式管理。

本功能適用於：

- Windows 10 和更新版本 (不包括 Windows 10 家用版)

NOTE

一旦符合 Intune 管理延伸模組必要條件，當 PowerShell 腳本或 Win32 應用程式指派給使用者或裝置時，就會自動安裝 Intune 管理延伸模組。如需詳細資訊，請參閱 [Intune 管理延伸模組必要條件](#)。

PowerShell 腳本在 WPI 裝置的工作場所加入 (未正式支援，可以部署到 WPI 裝置。具體而言，裝置內容 PowerShell 腳本可在 WPI 裝置上運作，但使用者內容 PowerShell 腳本的設計會予以忽略。WPI 裝置上會忽略使用者內容腳本，且不會向 Microsoft 端點管理員主控台報告。

移至新式管理

使用者運算正在經歷數位轉型。傳統 IT 著重於單一裝置平臺、企業擁有的裝置、從辦公室工作的使用者，以及不同的手動、回應式 IT 程式。新式工作場所使用許多屬於使用者和企業擁有的平臺。它可讓使用者從任何地方工作，並提供自動化和主動的 IT 程式。

MDM 服務，例如 Microsoft Intune，可以管理執行 Windows 10 的行動裝置和桌面裝置。內建 Windows 10 管理用戶端會與 Intune 通訊，以執行企業管理工作。您可能需要一些工作，例如進階裝置設定和疑難排解。針對 Win32 應用程式管理，您可以在 Windows 10 裝置上使用 [Win32 應用程式管理](#) 功能。

Intune 管理延伸模組可補充內建 Windows 10 MDM 功能。您可以建立要在 Windows 10 裝置上執行的 PowerShell 腳本。例如，建立執行進階裝置設定的 PowerShell 腳本。然後，將腳本上傳至 Intune、將腳本指派給 Azure Active Directory (AD) 群組，然後執行腳本。然後，您可以從開始到完成監視腳本的執行狀態。

開始之前

- 當腳本設定為使用者內容，且使用者具有系統管理員許可權時，PowerShell 腳本預設會以系統管理員許可權執行。
- 使用者不需要登入裝置即可執行 PowerShell 腳本。
- Intune 管理延伸模組代理程式會在每次重新開機後檢查是否有任何新的腳本或變更。將原則指派給 Azure AD 群組之後，就會執行 PowerShell 腳本，並報告執行結果。腳本執行之後，除非腳本或原則中有變更，否則不會再次執行。如果腳本失敗，Intune 管理延伸模組代理程式會針對接下來的三個連續 Intune 管理延伸模組代理程式簽入重試腳本三次。
- 針對共用裝置，PowerShell 腳本會針對每個登入的新使用者執行。
- PowerShell 腳本會在 Win32 應用程式執行之前執行。換句話說，PowerShell 腳本會先執行。然後，執行 Win32 應用程式。
- PowerShell 腳本會在 30 分鐘後逾時。

先決條件

Intune管理延伸模組具有下列必要條件。一旦符合，Intune管理延伸模組會在 PowerShell 腳本或 Win32 應用程式指派給使用者或裝置時自動安裝。

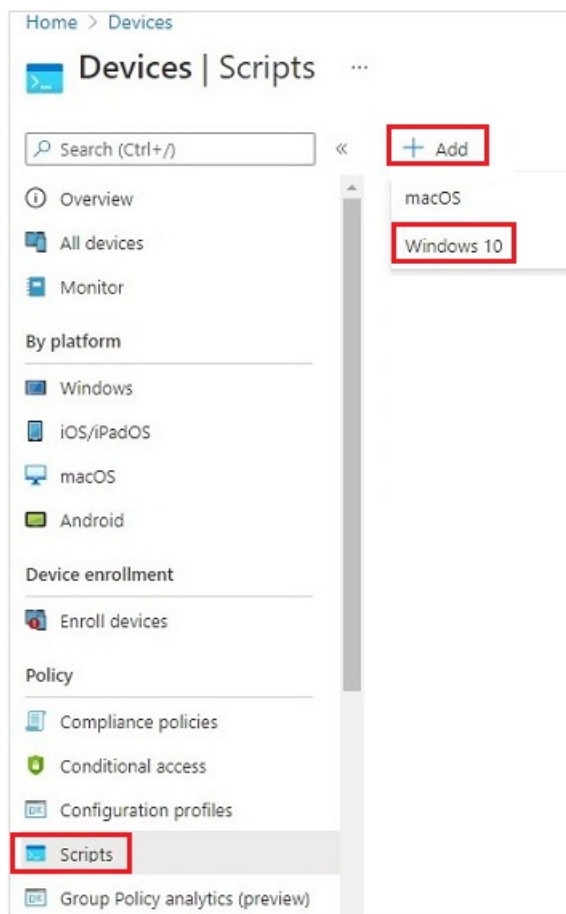
- 執行 Windows 10 1607 版或更新版本的裝置。如果裝置是使用[大量自動註冊](#)來註冊，則裝置必須執行 Windows 10 1709 版或更新版本。S 模式 Windows 10 不支援 Intune 管理延伸模組，因為 S 模式不允許執行非市集應用程式。
- 已加入 Azure Active Directory (AD) 的裝置，包括：
 - 已加入混合式 Azure AD 的裝置：已加入 Azure Active Directory (AAD)，也已加入 內部部署的 Active Directory (AD)。如需指引，請參閱 [規劃混合式 Azure Active Directory Join](#) 實作。
- 已註冊 Azure AD/加入工作場所 (WPI)：在 Azure Active Directory (AAD) 中 [註冊](#) 的裝置，如需詳細資訊，請參閱 [Workplace Join 作為順暢的第二因素驗證](#)。通常這些是自備裝置 (BYOD) 裝置，這些裝置已透過 [設定]>[帳戶]>[存取公司或學校] 新增公司或學校帳戶。
- 在 Intune 中註冊的裝置，包括：
 - 在群組原則中註冊的裝置 (GPO)。如需指引，請參閱[使用 群組原則 自動註冊 Windows 10 裝置](#)。
 - 在 Intune 中手動註冊的裝置，其時機如下：
 - 已在 Azure AD 中啟用[自動註冊 Intune](#)。使用者使用本機使用者帳戶登入裝置，並手動將裝置加入 Azure AD。然後，他們使用其 Azure AD 帳戶登入裝置。
- OR
- 使用者使用其 Azure AD 帳戶登入裝置，然後註冊 Intune。
- 使用 Configuration Manager 和 Intune 的共同管理裝置。安裝 Win32 應用程式時，請確定 [應用程式] 工作負載已設定為 [試驗 Intune 或 Intune]。即使 [應用程式] 工作負載設定為 [Configuration Manager]，也會執行 PowerShell 腳本。當您將 PowerShell 腳本目標設為裝置時，Intune 管理延伸模組將會部署到裝置。請記住，裝置必須是已加入 Azure AD 或混合式 Azure AD 的裝置。而且，它必須執行 Windows 10 1607 版或更新版本。如需指引，請參閱下列文章：
 - [什麼是共同管理](#)
 - [用戶端應用程式工作負載](#)
 - [如何將 Configuration Manager 工作負載切換至 Intune](#)
- 如果裝置的系統時鐘超過月份或年份的過期，部署至執行 Intune 管理延伸模組之用戶端的腳本將無法執行。一旦系統時鐘更新為最新狀態，腳本就會如預期般執行。

NOTE

如需使用 Window 10 VM 的相關資訊，請參閱[搭配使用 Windows 10 虛擬機器與 Intune](#)。

建立腳本原則並加以指派

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [裝置 > 腳本 > 新增 > Windows 10 及更新版本]。



3. 在 [基本] 中，輸入下列屬性，然後選取 [下一步]：

- **名稱**：輸入 PowerShell 腳本的名稱。
- **描述**：輸入 PowerShell 腳本的描述。這是選擇性設定，但建議進行。

4. 在 [腳本設定] 中，輸入下列屬性，然後選取 [下一步]：

- **腳本位置**：瀏覽至 PowerShell 腳本。腳本必須小於 200 KB (ASCII)。
- **使用登入的認證執行此腳本**：選取 [是] 以在裝置上以使用者的認證執行腳本。選擇 [否 (預設)] 在系統內容中執行腳本。許多系統管理員選擇 [是]。如果需要腳本才能在系統內容中執行，請選擇 [否]。
- **強制執行腳本簽章檢查**：如果腳本必須由受信任的發行者簽署，請選取 [是]。如果不需要簽署腳本，請選取 [否 (預設)]。
- **在 64 位 PowerShell 主機中執行腳本**：選取 [是] 以在 64 位用戶端架構的 64 位 PowerShell 主機上執行腳本。選取 [否 (預設)] 在 32 位 PowerShell 主機中執行腳本。

當設定為 [是] 或 [否] 時，請針對新的和現有的原則行為使用下表：

64 位元架構	32 位元架構	32 位元 PowerShell 主機	64 位元 PowerShell 主機
否	32 位元	支援 32 位 PowerShell 主機	只在 32 位 PowerShell 主機中執行，這適用於 32 位和 64 位架構。

是 64 位元	64 位元	32 位元	32 位元
是	64 位元	在 64 位 PowerShell 主機中執行 64 位架構的腳本。在 32 位上執行時，腳本會在 32 位的 PowerShell 主機中執行。	在 32 位 PowerShell 主機中執行腳本。如果此設定變更為 64 位，則腳本會開啟 (不會在 64 位 PowerShell 主機中執行)，並報告結果。在 32 位上執行時，腳本會在 32 位 PowerShell 主機中執行。

5. 選取 [範圍標籤]。範圍標籤是選擇性的。[使用角色型存取控制 \(RBAC\) 和分散式 IT 的範圍標籤](#) 具有詳細資訊。

若要新增範圍標籤：

- 選擇 [選取範圍標籤 > 從清單中選取現有的範圍標籤 > 選取]。
 - 完成時，選取 [下一步]。
6. 選取 [指派**][選取要包含的** > 群組]。系統會顯示現有的 Azure AD 群組清單。
- 選取一或多個群組，其中包含裝置接收腳本的使用者。選擇 [選取]。您選擇的群組會顯示在清單中，並會收到您的原則。

NOTE

Intune 中的 PowerShell 腳本可以以 Azure AD 裝置安全性群組或 Azure AD 使用者安全性群組為目標。不過，以加入工作場所 (WPI) 裝置為目標時，只能使用 Azure AD 裝置安全性群組，(使用者目標將) 忽略。如需詳細資訊，請參閱 [WPI 裝置的工作場所加入 \(Win32 應用程式支援\)](#)。

- 選取 [下一步]。

[Dashboard](#) > [Microsoft Intune](#) > [Device configuration - PowerShell scripts](#) > [Add PowerShell script](#)

Add PowerShell script

Basics
 Script settings
 Scope tags
 Assignments
 Review + add

+ Included groups

SELECTED GROUPS

GroupA	Remove
GroupB	Remove

[Select groups to include](#)

[Previous](#)

[Next](#)

7. 在 [檢閱 + 新增] 中，會顯示您設定的設定摘要。選取 [新增] 以儲存腳本。當您選取 [新增] 時，原則會部署到您選擇的群組。

無法執行腳本範例

上午 8 點

- 登記
- 執行腳本 ConfigScript01
- 腳本失敗

上午 9 點

- 登記
- 執行腳本 ConfigScript01
- 腳本失敗 (重試計數 = 1)

上午 10 點

- 登記
- 執行腳本 ConfigScript01
- 腳本失敗 (重試計數 = 2)

上午 11 點

- 登記
- 執行腳本 ConfigScript01
- 腳本失敗 (重試計數 = 3)

下午 12 點

- 登記
- 不會嘗試執行 ConfigScript01 腳本。
- 如果未對腳本進行其他變更，則不會嘗試執行腳本。

監視執行狀態

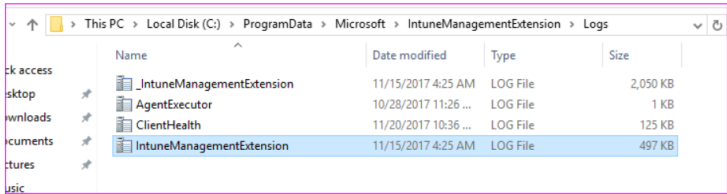
您可以在入口網站中監視使用者和裝置的 PowerShell 腳本執行狀態。

在 PowerShell 腳本中，選取要監視的腳本，選擇 [監視]，然後選擇下列其中一份報告：

- 裝置狀態
- 使用者狀態

Intune 管理延伸模組記錄

用戶端電腦上的代理程式記錄通常位於 `C:\ProgramData\Microsoft\IntuneManagementExtension\Logs`。您可以使用 [CMTrace.exe](#) 來檢視這些記錄檔。



Here is the path: `c:\programdata\microsoft\intunemanagementextension\logs`. You can download configMgr tools (cmtrace.exe) to view the log friendly and dynamically.

- IntuneManagementExtension.log is the main client log file, it contains all the agent check in, policy request, policy processing and reporting activities.
- AgentExecutor.log is the log file to track Powershell script execution details.
- ClientHealth.log is the log file to track sidecar agent client health activities

刪除腳本

在 PowerShell 腳本中，以滑鼠右鍵按一下腳本，然後選取 [刪除]。

常見問題和解決方案

問題：Intune管理延伸模組不會下載

可能的解決方法：

- 裝置未加入 Azure AD。請確定裝置符合本文) (的必要 條件。
- 沒有指派給使用者或裝置所屬群組的 PowerShell 腳本或 Win32 應用程式。
- 裝置無法簽入Intune服務。例如，沒有網際網路存取、無法存取 Windows 推播通知服務 (WNS) 等等。
- 裝置處於 S 模式。在 S 模式下執行的裝置不支援Intune管理延伸模組。

若要查看裝置是否已自動註冊，您可以：

1. 移至 [設定 > 帳戶 >] [存取公司或學校]。
2. 選取 [資訊] > 聯 結的帳戶。
3. 在 [進階診斷報告] 底下，選取 [建立報告]。
4. 在 `MDMDiagReport` 網頁瀏覽器中開啟。
5. 搜尋 `MDMDeviceWithAAD` 屬性。如果屬性存在，則會自動註冊裝置。如果此屬性不存在，則裝置不會自動註冊。

啟用Windows 10自動註冊包含在Intune中設定自動註冊的步驟。

問題：PowerShell 腳本未執行

可能的解決方法：

- PowerShell 腳本不會在每次登入時執行。它們會執行：
 - 將腳本指派給裝置時
 - 如果您變更腳本，請上傳腳本，並將腳本指派給使用者或裝置

TIP

Microsoft Intune 模組是在裝置上執行的服務，就像服務應用程式中列出的任何其他服務 (services.msc) 一樣。裝置重新開機之後，此服務也可能會重新開機，並使用 Intune 服務檢查是否有任何指派的 PowerShell 腳本。如果 Microsoft Intune 模組服務設定為 [手動]，則在裝置重新開機之後，服務可能不會重新開機。

- 請確定裝置已 加入 Azure AD。只有加入您工作場所或組織 (在 Azure AD 中 註冊) 的裝置將不會收到腳本。
- 確認Intune管理延伸模組已下載至 `%ProgramFiles(x86)%\Microsoft Intune Management Extension`。
- 腳本不會在 Surface Hub 上執行，也不會在 S 模式中Windows 10。
- 檢閱記錄中是否有任何錯誤。請參閱本文) 中的Intune管理延伸模組記錄 (。
- 針對可能的許可權問題，請確定 PowerShell 腳本的屬性已設定為 `Run this script using the logged on credentials`。另請檢查已登入的使用者是否具有執行腳本的適當許可權。
- 若要隔離腳本問題，您可以：
 - 檢閱您裝置上的 PowerShell 執行設定。如需指引，請參閱 PowerShell 執行 原則。
 - 使用 Intune 管理延伸模組執行範例腳本。例如，建立 `C:\Scripts` 目錄，並讓每個人完全掌控。執

行下列指令碼：

```
write-output "Script worked" | out-file c:\Scripts\output.txt
```

如果成功，應該建立output.txt，而且應該包含「腳本已運作」文字。

- 若要在不Intune的情況下測試腳本執行，請在本機使用[psexec 工具](#)在系統帳戶中執行腳本：

```
psexec -i -s
```

- 如果腳本回報成功，但實際上並未成功，則您的防毒軟體服務可能是沙箱化 AgentExecutor。下列腳本一律會回報Intune失敗。作為測試，您可以使用此腳本：

```
Write-Error -Message "Forced Fail" -Category OperationStopped  
mkdir "c:\temp"  
echo "Forced Fail" | out-file c:\temp\Fail.txt
```

如果腳本回報成功，請查看 `AgentExecutor.log` 以確認錯誤輸出。如果腳本執行，長度應該>2。

- 為了擷取 `.error` 和 `.output` 檔案，下列程式碼片段會透過 AgentExecutor 執行腳本至 PowerShell x86 () `C:\Windows\SysWOW64\WindowsPowerShell\v1.0`。它會保留記錄以供您檢閱。請記住，Intune管理延伸模組會在腳本執行之後清除記錄：

```
$scriptPath = read-host "Enter the path to the script file to execute"  
$logFolder = read-host "Enter the path to a folder to output the logs to"  
$outputPath = $logFolder+"\output.output"  
$errorPath = $logFolder+"\error.error"  
$timeoutPath = $logFolder+"\timeout.timeout"  
$timeoutVal = 60000  
$PSFolder = "C:\Windows\SysWOW64\WindowsPowerShell\v1.0"  
$AgentExec = "C:\Program Files (x86)\Microsoft Intune Management Extension\agentexecutor.exe"  
&$AgentExec -powershell $scriptPath $outputPath $errorPath $timeoutPath $timeoutVal $PSFolder  
0 0
```

後續步驟

[監視](#) 您的設定檔並 [進行疑難排解](#)。

在 Intune 中的 macOS 裝置上使用殼層腳本

2022/9/27 •

使用殼層腳本來擴充Intune中的裝置管理功能，超越 macOS 作業系統所支援的功能。

NOTE

Rosetta 2 必須在 Apple Silicon Mac 上執行 x64 (Intel) 版應用程式。若要在 Apple Silicon Mac 上自動安裝 Rosetta 2，您可以在 端點管理員 中部署殼層腳本。若要檢視範例腳本，請參閱 [Rosetta 2 安裝腳本](#)。

先決條件

請確定在撰寫殼層腳本並將它們指派給 macOS 裝置時，符合下列必要條件。

- 裝置正在執行 macOS 10.13 或更新版本。
- 裝置是由Intune管理。
- Shell 腳本開頭為 `#!`，且必須位於有效的位置，例如 `#!/bin/sh` 或 `#!/usr/bin/env zsh`。
- 已安裝適用殼層的命令列解譯器。

使用殼層腳本之前的重要考慮

- 殼層腳本需要在 macOS 裝置上成功安裝Microsoft Intune管理代理程式。如需詳細資訊，請參閱 [macOS Microsoft Intune管理代理程式](#)。
- 殼層腳本會以個別進程的形式在裝置上平行執行。
- 以登入使用者身分執行的殼層腳本，將會在執行時針對裝置上所有目前已登入的使用者帳戶執行。
- 使用者必須登入裝置，才能以登入使用者身分執行腳本。
- 如果腳本需要進行標準使用者帳戶無法進行變更，則需要根使用者權限。
- Shell 腳本會嘗試在特定情況下比所選腳本頻率更頻繁地執行，例如磁片已滿、儲存位置遭到竄改、本機快取遭到刪除，或 Mac 裝置重新開機時。

建立和指派殼層腳本原則

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [裝置 >] macOS > Shell 腳本 > [新增]。
3. 在 [基本] 中，輸入下列屬性，然後選取 [下一步]：
 - 名稱：輸入殼層腳本的名稱。
 - 描述：輸入殼層腳本的描述。這是選擇性設定，但建議進行。
4. 在 [腳本設定] 中，輸入下列屬性，然後選取 [下一步]：
 - 上傳腳本：流覽至殼層腳本。腳本檔案的大小必須小於 200 KB。
 - 以登入使用者身分執行腳本：選取 [是] 以在裝置上以使用者的認證執行腳本。選擇 [否 (預設)] 以根使用者身分執行腳本。
 - 隱藏裝置上的腳本通知：根據預設，每個執行的腳本都會顯示腳本通知。終端使用者會看到 *IT 正在從 macOS 裝置上的Intune設定您的電腦通知*。
 - 腳本頻率：選取執行腳本的頻率。選擇 [未設定 (預設)] 只執行腳本一次。
 - 腳本失敗時重試的次數上限：選取腳本傳回非零結束代碼時應該執行的次數，(零表示成功)。選擇 [

未設定 (預設) 在腳本失敗時不重試。

- 在 [範圍標籤] 中，選擇性地新增腳本的範圍標籤，然後選取 [下一步]。您可以使用範圍標籤來判斷誰可以在 Intune 中看到腳本。如需範圍標籤的完整詳細資料，請 [參閱針對分散式 IT 使用角色型存取控制和範圍標籤](#)。
- 選取 [指派**][選取要包含的** > 群組]。系統會顯示現有的 Azure AD 群組清單。選取要接收腳本的一或多個使用者或裝置群組。選擇 [選取]。您選擇的群組會顯示在清單中，並會接收您的腳本原則。

NOTE

- 指派給使用者群組的殼層腳本適用於任何登入 Mac 的使用者。
- 更新殼層腳本的指派也會更新適用於 macOS 的 Microsoft Intune MDM 代理程式指派。

- 在 [檢閱 + 新增] 中，會顯示您設定的設定摘要。選取 [新增] 以儲存腳本。當您選取 [新增] 時，腳本原則會部署到您選擇的群組。

您建立的腳本現在會出現在腳本清單中。如有需要，您可以在將 macOS 殼層腳本上傳至 Intune 之後，檢視這些腳本的內容。

監視殼層腳本原則

您可以選擇下列其中一份報告，監視使用者和裝置所有指派腳本的執行狀態：

- 腳本 > 選取要監視 > 的腳本 裝置狀態
- 腳本 > 選取要監視 > 的腳本 使用者狀態

IMPORTANT

不論選取的  為何，只有在腳本第一次執行時才會報告腳本執行狀態。後續執行時不會更新腳本執行狀態。不過，更新的腳本會被視為新的腳本，並會再次報告執行狀態。

腳本執行之後，它會傳回下列其中一個狀態：

- 腳本執行狀態為 Failed 表示腳本傳回非零結束代碼，或腳本格式不正確。
- 腳本執行狀態 為 Success 表示腳本傳回零做為結束代碼。

使用記錄收集對 macOS 殼層腳本原則進行疑難排解

您可以收集裝置記錄檔，以協助針對 macOS 裝置上的腳本問題進行疑難排解。

記錄收集的需求

在 macOS 裝置上收集記錄需要下列專案：

- 您必須指定完整的絕對記錄檔路徑。
- 檔案路徑只能使用分號 (;) 分隔。
- 要上傳的記錄收集大小上限為 60 MB (壓縮) 或 25 個檔案，以先發生者為準。
- 記錄收集允許的檔案類型包含下列副檔名：.log、.zip、.gz、.tar、.txt、.xml、.crash、.rtf

收集裝置記錄

- 登入 [Microsoft 端點管理員系統管理中心](#)。
- 流覽至 [裝置 > 腳本]，然後選取 macOS 殼層腳本。
- 在 [裝置狀態] 或 [使用者狀態 報告] 中，選取裝置。

4. 選取 [收集記錄]，提供僅以分號分隔的記錄檔資料夾路徑 (:) 路徑之間沒有空格或分行符號。

例如，多個路徑應該寫入為 `/Path/to/logfile1.zip;/Path/to/logfile2.log`。

IMPORTANT

使用逗號、句號、分行符號或不含空格的引號分隔的多個記錄檔路徑，將會導致記錄檔收集錯誤。路徑之間也不允許空格做為分隔符號。

5. 選取 [確定]。下次裝置上的Intune管理代理程式使用 Intune 簽入時，就會收集記錄。此簽入通常每 8 小時發生一次。

NOTE

- 收集的記錄會在裝置上加密、傳輸並儲存在 Microsoft Azure 儲存體中 30 天。預存記錄會視需要解密，並使用 Microsoft 端點管理員 系統管理中心下載。
- 除了系統管理員指定的記錄之外，也會從下列資料夾收集Intune管理代理程式記錄：和 `~/Library/Logs/Microsoft/Intune`。 `/Library/Logs/Microsoft/Intune` 代理程式記錄檔名稱為 `IntuneMDMDaemon date--time.log` 和 `IntuneMDMAgent date--time.log`。
- 如果遺漏任何系統管理員指定的檔案或副檔名錯誤，您會發現中 `LogCollectionInfo.txt` 列出這些檔案名。

記錄收集錯誤

記錄收集可能因為下表中提供的下列任何原因而無法成功。若要解決這些錯誤，請遵循補救步驟。

錯誤 (ID)	錯誤 (DEC)	錯誤	錯誤
0X87D300D1	2016214834	記錄檔大小不能超過 60 MB。	請確定壓縮的記錄大小小於 60 MB。
0X87D300D1	2016214831	提供的記錄檔路徑必須存在。系統使用者資料夾是記錄檔的無效位置。	確定提供的檔案路徑有效且可存取。
0X87D300D2	2016214830	記錄收集檔案上傳失敗，因為上傳 URL 到期。	重試 [■] 動作。
0X87D300D3、 0X87D300D5、 0X87D300D7	2016214829, 2016214827, 2016214825	記錄收集檔案上傳失敗，因為加密失敗。重試記錄上傳。	重試 [■] 動作。
	2016214828	記錄檔數目超過允許的 25 個檔案限制。	一次最多隻能收集 25 個記錄檔。
0X87D300D6	2016214826	記錄收集檔案上傳失敗，因為 zip 錯誤。重試記錄上傳。	重試 [■] 動作。
	2016214740	因為找不到壓縮的記錄，所以無法加密記錄。	重試 [■] 動作。
	2016214739	已收集記錄，但無法儲存。	重試 [■] 動作。

macOS 的自訂屬性

您可以建立自訂屬性設定檔，讓您可以使用殼層腳本從受控 macOS 裝置收集自訂屬性。

建立並指派 macOS 裝置的自訂屬性

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [裝置 >] macOS > [自訂屬性 >][新增]。
3. 在 [基本] 中，輸入下列屬性，然後選取 [下一步]：
 - 名稱：輸入腳本的名稱。
 - 描述：輸入腳本的描述。這是選擇性設定，但建議進行。
4. 在 [屬性設定] 中，輸入下列屬性，然後選取 [下一步]：
 - 屬性的資料類型：選取腳本傳回之結果的資料類型。可用的值為 String、Integer 和 Date。
 - 腳本：選取腳本檔案。

其他詳細資料：

- 殼層腳本必須回應要報告的屬性，而且輸出的資料類型必須符合自訂屬性設定檔中屬性的資料類型。
- 殼層腳本傳回的結果必須是 20 KB 或更少。

NOTE

使用 類型屬性時，請確定殼層腳本會以 ISO-8601 格式傳回日期。請參閱下列範例。

■■■■ ISO-8601 ■■■■:

```
#!/bin/sh
var=$(date +"%Y-%m-%dT%H:%M:%S%z")
echo $var # Prints an ISO-8601 compliant date with time-zone
```

■■ UTC ■■■ ISO-8601 ■■■:

```
#!/bin/sh
var=$(date -u +"%Y-%m-%dT%H:%M:%SZ")
echo $var # Prints an ISO-8601 compliant date in UTC time
```

5. 在 [指派] 中，按一下 [選取要包含的群組]。當您選擇 [選取要包含 現有 Azure AD 群組清單的群組] 時，會顯示。選取要接收腳本的一或多個使用者或裝置群組。選擇 [選取]。您選擇的群組會顯示在清單中，並會接收您的腳本原則。或者，您可以在 [指派 給] 旁的下拉式方塊中選取其中一個選項，選擇選取 [所有使用者]、[所有裝置] 或 [所有使用者和所有裝置]。

NOTE

- 指派給使用者群組的腳本適用於任何登入 Mac 的使用者。

6. 在 [檢閱 + 新增] 中，會顯示您設定的設定摘要。選取 [新增] 以儲存腳本。當您選取 [新增] 時，腳本原則會部署到您選擇的群組。

您建立的腳本現在會出現在自訂屬性清單中。如有需要，您可以在將自訂屬性上傳至Intune之後，檢視這些屬性的內容。

監視自訂屬性原則

您可以選擇下列其中一份報告，監視使用者和裝置的所有已指派自訂屬性設定檔的執行狀態：

- 自訂屬性 > 選取要監視的自訂屬性設定檔 > 裝置狀態
- 自訂屬性 > 選取要監視的自訂屬性設定檔 > 使用者狀態

IMPORTANT

自訂屬性設定檔中提供的殼層腳本會每隔 8 小時在受控 Mac 上執行一次並回報。

自訂屬性設定檔執行之後，它會傳回下列其中一個狀態：

- [失敗] 狀態表示腳本傳回非零結束代碼，或腳本格式不正確。此錯誤會在 [結果] 資料行中報告。
- 當狀態為 Success 時，表示腳本傳回零做為結束代碼。腳本所回應的輸出會在 [結果] 資料行中回報。

常見問題集

為什麼指派的殼層腳本未在裝置上執行？

可能有幾個原因：

- 代理程式可能需要簽入才能接收新的或更新的腳本。此簽入程式每隔 8 小時會發生一次，而且與 MDM 簽入不同。請確定裝置已喚醒並聯機到網路，以便代理程式成功簽入，並等候代理程式簽入。您也可以要求終端使用者在 Mac 上開啟公司入口網站、選取裝置，然後按一下 [檢查設定]。
- 可能未安裝代理程式。檢查代理程式是否已安裝在 `/Library/Intune/Microsoft Intune Agent.app` macOS 裝置上。
- 代理程式可能不是處於狀況良好的狀態。代理程式會嘗試復原 24 小時、移除本身，並在仍然指派殼層腳本時重新安裝。

腳本執行狀態報表的頻率為何？

腳本執行完成後，就會將腳本執行狀態回報給 Microsoft 端點管理員 管理員 主控台。如果腳本排定以設定頻率定期執行，則只會在第一次執行時報告狀態。

殼層腳本何時會再次執行？

只有在設定 腳本失敗 設定且腳本在執行時失敗時，才會再次執行腳本。重試的次數上限。如果未設定 腳本失敗且腳本 在執行時失敗，則重試的次數上限不會再次執行，且執行狀態會回報為 失敗。

殼層腳本需要哪些Intune角色許可權？

指派的 intune 角色需要 裝置設定 許可權，才能刪除、指派、建立、更新或讀取殼層腳本。

已知問題

- 沒有腳本執行狀態：在裝置上收到腳本且裝置在回報執行狀態之前離線的不太可能情況下，裝置不會在管理主控台中報告腳本的執行狀態。

其他資訊

當您從 Microsoft 端點管理員 部署 macOS 裝置的殼層腳本或自訂屬性時，它會部署在 Apple Silicon Mac 電腦上以原生方式執行之 Intune 管理代理程式應用程式的新通用版本。相同的部署會在 Intel Mac 電腦上安裝 x64 版本的應用程式。Rosetta 2 必須在 Apple Silicon Mac 上執行 x64 (Intel) 版應用程式。若要在 Apple Silicon Mac 上自動安裝 Rosetta 2，您可以在 端點管理員 中部署殼層腳本。若要檢視範例腳本，請參閱 [Rosetta 2 安裝腳本](#)。

後續步驟

- [在 Microsoft Intune 中建立合規性](#)

使用 Microsoft Intune 將應用程式指派給群組

2022/9/27 •

將**應用程式**新增至Microsoft Intune之後，您可以將應用程式指派給使用者和裝置。請務必注意，無論裝置是否由Intune管理，您都可以將應用程式部署到裝置。

NOTE

將 Android Enterprise (完全受控裝置的目標設為 COBO) 和 Android Enterprise 公司擁有的個人 () 裝置時，使用者 ■ 和 ■ 支援「■ 的裝置」部署意圖。

下表列出 **將應用程式指派給** 使用者和裝置的各種選項：

■	■ INTUNE ■■■■	■ INTUNE ■■■■
指派給使用者	是	是
指派給裝置	是	否
指派已包裝的應用程式或應用程式, 併入應用程式保護原則的Intune SDK ()	是	是
將應用程式指派為可用	是	是
將應用程式指派為必要專案	是	否
卸載應用程式	是	否
從 Intune 接收應用程式更新	是	否
終端使用者從公司入口網站應用程式安裝可用的應用程式	是	否
終端使用者會從網頁型公司入口網站安裝可用的應用程式	是	是

NOTE

目前，您可以將 iOS/iPadOS 和 Android 應用程式指派 (企業營運和市集購買的應用程式,) 指派給未向Intune註冊的裝置。

若要在未向 Intune 註冊的裝置上收到應用程式更新，裝置使用者必須前往其組織的公司入口網站，然後手動安裝應用程式更新。

可用的指派 僅適用於使用者群組，而非裝置群組。

如果在 Android Enterprise 個人擁有的工作設定檔裝置上，如有需要指派受控 Google Play 生產前追蹤應用程式，它們將不會安裝在裝置上。若要解決這個問題，請建立兩個相同的使用者群組，並將生產前曲目指派為「可用」給其中一個，並將「必要」指派給另一個。結果是生產前追蹤會成功部署到裝置。

指派應用程式

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式] > [所有應用程式]。
3. 在 [應用程式] 窗格中，選取您要指派的應用程式。
4. 在功能表的 [管理] 區段中，選取 [指派]。
5. 選取 [新增群組] 以開啟與應用程式相關的 [新增群組] 窗格。
6. 針對特定應用程式，選取指派類型：
 - **適用於已註冊的裝置**：將應用程式指派給可從公司入口網站應用程式或網站安裝應用程式的使用者群組。
 - **不需註冊即可使用**：將此應用程式指派給裝置未向Intune註冊的使用者群組。使用者必須獲指派Intune授權，請參閱[Intune授權](#)。
 - **必要**：應用程式會安裝在所選群組中的裝置上。某些平臺可能會有額外的提示，讓終端使用者在應用程式安裝開始之前確認。
 - **卸載**：如果Intune先前已透過使用相同部署的「適用於已註冊的裝置」或「必要」指派將應用程式安裝到裝置上，則會從選取群組中的裝置卸載應用程式。

NOTE

■ iOS/iPadOS ■：

- 若要設定當裝置不再受管理時，受控應用程式會發生什麼情況，您可以在裝置 ■ 選取 [卸載] 底下的預定設定。如需詳細資訊，請參閱 [iOS/iPadOS 受控應用程式的應用程式卸載設定](#)。
- 如果您已建立包含個別應用程式 VPN 設定的 iOS/iPadOS VPN 設定檔，您可以在 VPN ■ VPN 設定檔。執行應用程式時，會開啟 VPN 連線。如需詳細資訊，請參閱 [iOS/iPadOS 裝置的 VPN 設定](#)。
- 若要設定使用者是否將必要的 iOS/iPadOS 應用程式安裝為抽取式應用程式，您可以選取 [■] 底下的設定。

■ Android ■：

- 如果您將 Android 應用程式部署為 [■]，報告狀態將僅適用於已註冊的裝置。

■ [■]：

- 只有在登入公司入口網站的使用者是註冊裝置的主要使用者，且應用程式適用於裝置時，應用程式才會顯示為可用。

7. 若要選取受此應用程式指派影響的使用者群組，請選取 [包含的群組]。
8. 選取要包含的一或多個群組之後，請選取 [選取]。
9. 在 [指派] 窗格中，選取 [確定] 以完成包含的群組選取。
10. 如果您想要排除任何使用者群組不受此應用程式指派影響，請選取 [排除群組]。
11. 如果您已選擇排除任何群組，請在 [選取群組] 中選取 [選取]。
12. 在 [新增群組] 窗格中，選取 [確定]。
13. 在 [應用程式 指派] 窗格中，選取 [儲存]。

應用程式現在會指派給您選取的群組。如需包含和排除應用程式指派的詳細資訊，請參閱 [包含和排除應用程式指派](#)。

TIP

Intune也支援將應用程式指派給巢狀群組。例如，如果您將應用程式指派給「工程通用」群組，並以「工程 APAC」、「工程 EMEA」和「工程美國」巢狀為子群組，則這些子群組的成員也會以指派為目標。

如何解決應用程式意圖之間的衝突

單一群組無法以多個應用程式指派意圖為目標，不過，如果使用者或裝置是多個群組的成員，且每個群組都以不同的意圖指派，則會導致衝突。不建議為應用程式建立指派衝突。下表中的資訊可協助您瞭解發生衝突時所產生的意圖：

「1」	「2」	結果
需要使用者	使用者可用	必要和可用
需要使用者	使用者卸載	必要
使用者可用	使用者卸載	解除安裝
需要使用者	需要裝置	兩者都存在，Intune處理必要專案
需要使用者	裝置卸載	兩者都存在，Intune解決必要
使用者可用	需要裝置	兩者都存在，Intune解析必要 (和可用)
使用者可用	裝置卸載	兩者都存在，Intune解析 [可用]。 應用程式會顯示在公司入口網站中。 如果應用程式已安裝 (為具有先前意圖) 的必要應用程式，則會卸載應用程式。 如果使用者  選取 [安裝]，則會安裝應用程式，且不接受卸載意圖。
使用者卸載	需要裝置	兩者都存在，Intune解決必要
使用者卸載	裝置卸載	兩者都存在，Intune解析卸載
需要裝置	裝置卸載	必要
使用者必要且可用	使用者可用	必要和可用
使用者必要且可用	使用者卸載	必要和可用
使用者必要且可用	需要裝置	同時存在、必要和可用
使用者必要且可用	裝置卸載	兩者都存在，Intune解析必要 (和可用)
使用者不需註冊即可使用	使用者必要且可用	必要和可用
使用者不需註冊即可使用	需要使用者	必要

1	2	
使用者不需註冊即可使用	使用者可用	可以使用
使用者不需註冊即可使用	需要裝置	必要且不註冊即可使用
使用者不需註冊即可使用	裝置卸載	卸載且不需註冊即可使用。 如果使用者未從公司入口網站安裝應用程式，則會接受卸載。 如果使用者從公司入口網站安裝應用程式，安裝會優先於卸載。

NOTE

僅適用於受控 iOS 市集應用程式，當您將這些應用程式新增至 Microsoft Intune，並將其指派為 **■** 時，會自動建立具有 **■** 和 **■** 意圖的應用程式。

iOS 市集應用程式 (非 iOS/iPadOS VPP 應用程式) 在裝置簽入時，會在裝置上強制執行以必要意圖為目標的應用程式，也會顯示在公司入口網站應用程式中。

當裝置 **■** **■** 中發生衝突時，當裝置不再受管理時，不會從裝置移除應用程式。

NOTE

部署為公司擁有之工作設定檔裝置所需之應用程式無法由使用者手動卸載。

將受控 Google Play 應用程式部署至非受控裝置

對於未註冊的 Android 裝置，您可以使用受控 Google Play 將市集應用程式和企業營運 (LOB) 應用程式部署給使用者。部署之後，您可以使用 [行動應用程式管理 \(MAM\)](#) 來管理應用程式。受控 Google Play 應用程式目標為 **[無論是否可註冊]** 都會出現在終端使用者裝置上的 Play Store 應用程式中，而不是在公司入口網站應用程式中。終端使用者會從 Play 應用程式以這種方式流覽和安裝部署的應用程式。由於應用程式是從受控 Google Play 安裝的，因此終端使用者不需要變更其裝置設定，即可允許從未知來源安裝應用程式，這表示裝置將會更安全。如果應用程式開發人員將安裝在使用者裝置上的新版應用程式發佈至 Play，則 Play 會自動更新應用程式。

將受控 Google Play 應用程式指派給非受控裝置的步驟：

1. 將您的Intune租使用者連線到受控 Google Play。如果您已經這麼做來管理 Android Enterprise 個人擁有、專用、完全受控或公司擁有的工作設定檔裝置，則不需要再執行一次。
2. 從受控 Google Play 將應用程式新增至Intune主控台。
3. 以受控 Google Play 應用程式為目標，無論是否向所需的使用者群組 **註冊都可** 使用。**未** 註冊的裝置不支援必要和 **卸載** 應用程式目標。
4. 將應用程式保護原則指派給使用者群組。
5. 使用者記錄在任何受保護的應用程式中。
6. 下次使用者開啟公司入口網站應用程式並完成登入程式時，他們會在 [應用程式] 區段中看到一則訊息，指出有應用程式可供他們使用。使用者可以選取此通知來流覽至 Play Store。

NOTE

您可以將 [裝置註冊設定選項](#) 設定為 ☐ ☒ 或 ☐。此設定可防止使用者在登入公司入口網站之後，無意中註冊其裝置，或收到註冊其裝置的通知。

- 終端使用者可以展開 Play Store 應用程式內的操作功能表，並切換其個人 Google 帳戶 (看到其個人應用程式) 的位置，以及其工作帳戶 (其中，他們會看到以他們為目標的市集和 LOB 應用程式)。終端使用者會點選 [\[在 Play Store 應用程式中安裝\]](#) 來安裝應用程式。

當應用程式選擇性抹除在Intune主控台中發出時，工作帳戶將會自動從 Play Store 應用程式中移除，而使用者會從該時間點看到 Play Store 應用程式目錄中的工作應用程式。從裝置移除工作帳戶時，從 Play Store 安裝的應用程式會保留在裝置上，且不會卸載。

iOS 受控應用程式的應用程式卸載設定

針對 iOS/iPadOS 裝置，您可以選擇將裝置從Intune取消註冊，或在 [裝置移除設定上使用 \[卸載\]](#) 移除管理設定檔時，受控應用程式會發生什麼情況。此設定僅適用於註冊裝置並以受控方式安裝應用程式之後的應用程式。無法為 Web 應用程式或 Web 連結設定此設定。只有行動應用程式管理 (MAM) 所保護的資料會在應用程式選擇性抹除淘汰之後移除。

新指派會預先填入設定的預設值，如下所示：

IOS 設定	[設定] 設定
企業營運應用程式	是
市集應用程式	否
VPP 應用程式	否
內建應用程式	否

NOTE

是：如果您要將此設定更新為「適用於已註冊的裝置」或「可使用或不含註冊」群組，則在使用者同步裝置與Intune並重新安裝應用程式之前，已擁有受控應用程式的使用者將不會取得更新的設定。

否：應用程式卸載設定是在 2019 年 5 月導入。在此日期之前存在的指派未修改，而且所有受控應用程式都會在裝置從管理中移除時移除。如果您的指派是在 2019 年 5 月之前建立，您可能需要明確設定應用程式卸載設定，因為上述預設設定可能不適用。

後續步驟

若要深入瞭解監視應用程式指派，請參閱 [如何監視應用程式](#)。

在 Microsoft Intune 中包含和排除應用程式指派

2022/9/27 •

在 Intune 中，您可以指派要包含和排除的使用者群組，以判斷誰可以存取應用程式。將群組指派給應用程式之前，您必須設定應用程式的指派類型。指派類型可讓應用程式可供使用、必要或卸載應用程式。

若要設定應用程式的可用性，您可以使用包含和排除群組指派的組合，來包含和排除使用者或裝置群組的應用程式指派。當您藉由包含大型群組來提供應用程式，然後藉由排除較小的群組來縮小選取的使用者範圍時，這項功能會很有用。較小的群組可能是測試群組或執行群組。

最佳做法是特別為您的使用者群組建立和指派應用程式，並分別為您的裝置群組指派應用程式。如需群組的詳細資訊，請 [參閱新增群組以組織使用者和裝置](#)。

包含或排除應用程式指派時存在重要案例：

- 排除優先於包含在下列相同群組類型案例中：

- 指派應用程式時包含使用者群組和排除使用者群組
- 指派應用程式時包含裝置群組和排除裝置群組

例如，如果您將裝置群組指派給 [所有公司使用者] 使用者群組，但排除 [資深管理人員] 使用者群組中的成員，則除了資深管理人員以外的所有公司使用者都會取得指派，因為這兩個群組都是使用者群組。

- Intune 不會評估使用者對裝置群組的關聯性。如果您將應用程式指派給混合群組，結果可能不是您想要或預期的結果。

例如，如果您將裝置群組指派給 [所有使用者] 使用者群組，但排除 [所有個人裝置] 裝置群組。在此混合群組應用程式指派中，所有使用者都會取得應用程式。排除範圍不適用。

因此，不建議將應用程式指派給混合群組。

NOTE

當您設定應用程式的群組指派時，「包含」類型已被取代，並取代為排除群組功能。

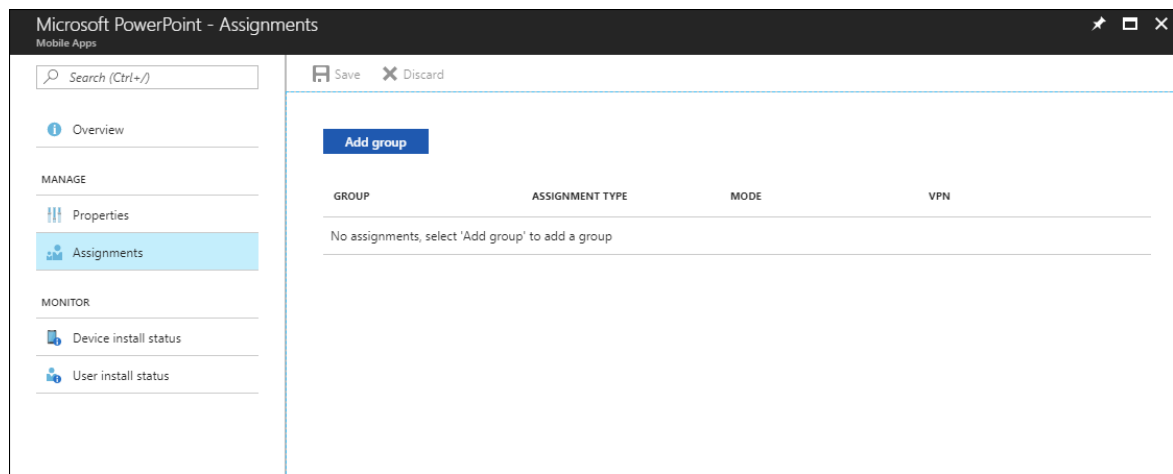
Intune 會在主控台中提供預先建立 [所有使用者] 和 [所有裝置] 群組。為了方便起見，這些群組具有內建的優化。強烈建議您使用這些群組以所有使用者和所有裝置為目標，而不是您可能會自行建立的任何「所有使用者」或「所有裝置」群組。

Android 企業支援包含和排除群組。您可以利用內建的 [所有 Android 裝置] 和 [所有 Android 使用者] 群組來指派 Android 企業應用程式。

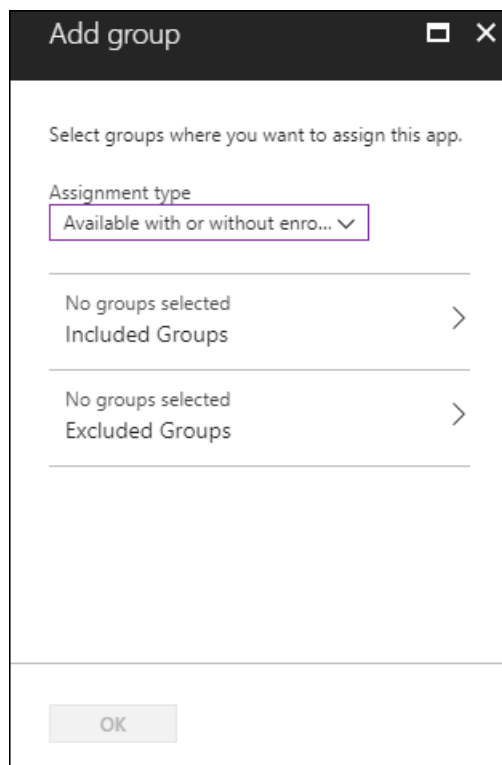
指派應用程式時包含和排除群組

若要使用包含和排除指派將應用程式指派給群組：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式] > [所有應用程式]。新增的應用程式清單會顯示。
3. 選取您要指派的應用程式。儀表板會顯示應用程式的相關資訊。
4. 在功能表的 [管理] 區段中，選取 [指派]。



5. 選取 [新增群組] 以新增獲指派應用程式的使用者群組。
6. 在 [新增群組] 窗格中，從可用的指派類型中選取 [指派類型]。
7. 針對指派類型，選取 [有或不註冊即可使用]。



8. 選取 [包含的群組] 以選取您要讓此應用程式可供使用的使用者群組。

NOTE

當您新增群組時，如果特定指派類型已包含任何其他群組，則會預先選取應用程式，而且無法針對其他 Include 指派類型進行修改。已使用的群組無法當做包含的群組使用。

9. 選取 [是] 讓所有使用者都能使用此應用程式。

Add group

Assign

Select groups where you want to assign this app.

Assignment type

Available with or without enro... ▼

No groups selected
Included Groups

No groups selected
Excluded Groups

OK

Groups that have already been assigned or selected are disabled. To select a disabled group, remove it from this app's assigned list

Select the groups where you want to make this app available with or without enrollment. If you select a VPN profile, you need to assign it to the same groups as this app.

All users

Make this app available to all users, regardless of whether their devices are enrolled in Intune Yes No

Selected groups

Select groups to include

GROUP

No groups selected

OK

10. 選取 [確定] 以設定要包含的群組。
11. 選取 [排除的群組] 以選取您想要讓此應用程式無法使用的使用者群組。
12. 選取要排除的群組。這會讓這些群組無法使用此應用程式。

Add group

Select groups

Azure AD groups

Select groups where you want to assign this app.

Assignment type

Available with or without enro... ▼

1 group selected
Included Groups

No groups selected
Excluded Groups

OK

+ Invite

Select

Search by name or email address ✓

AD Admin

FP Full PC Client

☒ AP AppTesters

Selected
AppTesters

Select

13. 選取 [選取] 以完成您的群組選取。

14. 在 [新增群組] 窗格中，選取 [確定]。應用程式指派清單隨即出現。

15. 按一下 [儲存] 讓您的群組指派成為應用程式的使用中。

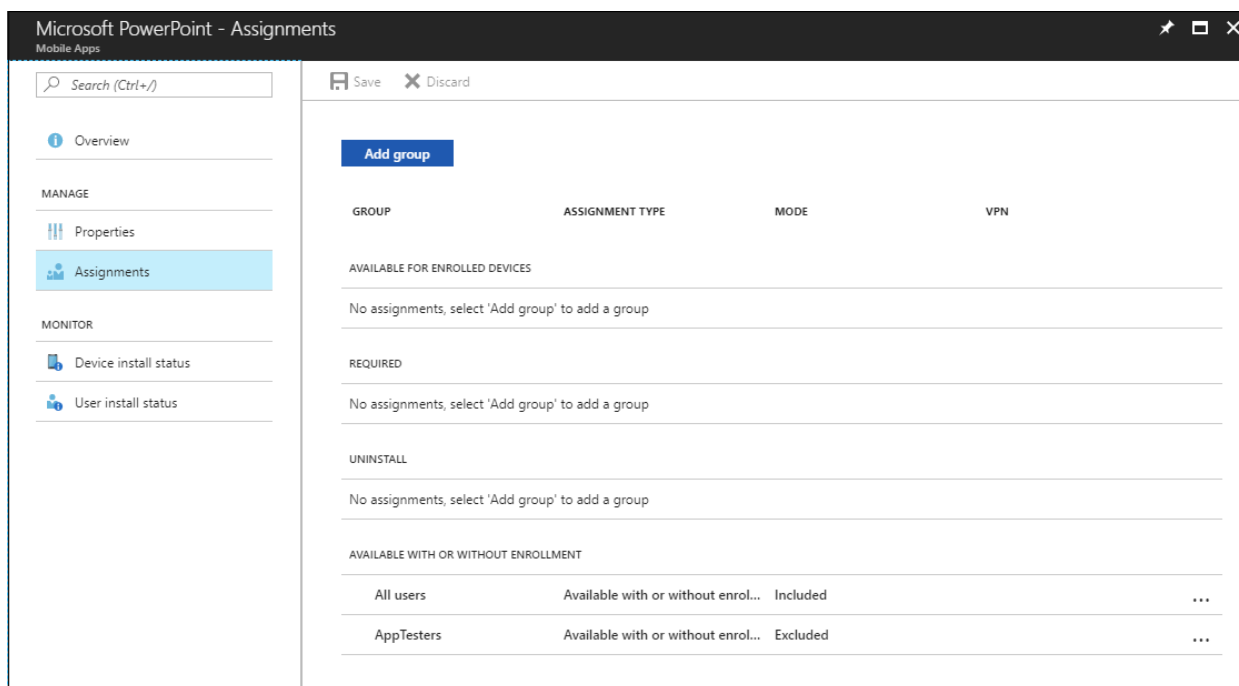
當您進行群組指派時，無法修改已指派的群組。如果您想要選取目前無法使用的群組，請先從應用程式的指派清單中移除應用程式。

若要編輯指派，請在應用程式的 [指派] 清單中，選取包含您要變更之特定指派的資料列。您也可以選取資料列結尾的省略號 (...)，然後選取 [移除]，以移除指派。

NOTE

移除群組指派不會移除相關的應用程式，但 Android Enterprise專用、完全受控和公司擁有的工作設定檔裝置除外。已安裝的應用程式會保留在裝置上。

若要變更 [指派] 清單的檢視，請依 [指派類型] 或 [包含/排除] 分組。



The screenshot shows the 'Microsoft PowerPoint - Assignments' window. On the left is a sidebar with a search bar and navigation links: Overview, MANAGE (Properties, Assignments), and MONITOR (Device install status, User install status). The main area has 'Save' and 'Discard' buttons at the top. Below is an 'Add group' button. The main content is a table with columns: GROUP, ASSIGNMENT TYPE, MODE, and VPN. The table is divided into sections: AVAILABLE FOR ENROLLED DEVICES, REQUIRED, UNINSTALL, and AVAILABLE WITH OR WITHOUT ENROLLMENT. Each section currently shows 'No assignments, select 'Add group' to add a group'. The bottom section, 'AVAILABLE WITH OR WITHOUT ENROLLMENT', contains two rows of data.

GROUP	ASSIGNMENT TYPE	MODE	VPN
AVAILABLE FOR ENROLLED DEVICES			
No assignments, select 'Add group' to add a group			
REQUIRED			
No assignments, select 'Add group' to add a group			
UNINSTALL			
No assignments, select 'Add group' to add a group			
AVAILABLE WITH OR WITHOUT ENROLLMENT			
All users	Available with or without enrol...	Included	...
AppTesters	Available with or without enrol...	Excluded	...

後續步驟

- 如需包含和排除應用程式群組指派的詳細資訊，請參閱[Microsoft Intune部落格](#)。
- 瞭解如何 [監視應用程式資訊和指派](#)。

使用 Microsoft Intune Windows 10/11 應用程式部署

2022/9/27 •

Microsoft Intune 在 Windows 10 裝置上支援各種應用程式類型和部署案例。在您將應用程式新增至 Intune 後，您可以將應用程式指派給使用者和裝置。本文提供有關支援的 Windows 10 案例的詳細資料，也涵蓋當您將應用程式部署至 Windows 時所需注意的重要細節。如需部署應用程式（也稱為指派應用程式）的詳細資訊，請參閱 [將應用程式指派](#) 給群組。

企業營運 (LOB) 應用程式和商務用 Microsoft Store 應用程式是 Windows 10 裝置上支援的應用程式類型。Windows 應用程式的副檔名包括 .msi、.appx 及 .appxbundle。

NOTE

若要部署現代應用程式，您至少需要：

- 針對 Windows 10 1803，年5月23日 2018-KB4100403 (OS 組建 17134.81)。
- 針對 Windows 10 1709，2018 年6月21日-KB4284822 (OS 組建 16299.522)。

只有在沒有主要使用者關聯時，才 Windows 10 1803 和更新版本支援安裝應用程式。

執行 Windows 10 家用版版本的裝置不支援 LOB 應用程式部署。

支援的 Windows 10 應用程式類型

根據使用者執行的 Windows 10 版本，支援特定的應用程式類型。下表提供應用程式類型及 Windows 10 支援性。

	HOME	SS	BUSINESS	SS	SS	SS	HOLOLENS 1	SURFACE HUB	WCOS	SS
.MSI	否	是	是	是	是	否	否	否	否	否
.Intune Win	否	是	是	是	是	19H2 +	否	否	否	否
Office C2R	否	是	是	是	是	RS4 +	否	否	否	否
LOB: APPX/MSIX	是	是	是	是	是	是	是	是	是	是
MSFB 離線	是	是	是	是	是	是	是	是	是	是
線上 MSFB	是	是	是	是	是	是	RS4 +	否	是	是
Web App	是	是	是	是	是	是	是 ²	是 ²	是	是 ²

	HOME		BUSINESS			S	HOLOLENS	SURFACE HUB	WCOS	
儲存區連結	是	是	是	是	是	是	是	是	是	是
Microsoft Edge	否	是	是	是	是	19H2 + ³	否	否	否	否

¹若要解除鎖定應用程式管理，請將您的 HoloLens 裝置升級為[全息版的企業版](#)。

²僅從公司入口網站啟動。

³若要成功安裝 Edge app，裝置也必須被指派 S 模式原則。

NOTE

所有 Windows 的應用程式類型都需要註冊。

Windows 10 LOB 應用程式

您可以對 Intune 管理主控台進行 Windows 10 的 LOB 應用程式的簽署和上傳。這些可包含新式應用程式，例如通用 Windows 平臺 (UWP) 應用程式和 Windows 應用程式套件 (AppX)，以及 Win 32 應用程式，例如簡易 Microsoft Installer 套件檔案 (MSI)。管理員必須手動上傳和部署 LOB 應用程式的更新。這些更新會自動安裝在已安裝應用程式的使用者裝置上。不需要使用者介入，使用者也無法控制更新。

商務用 Microsoft Store 應用程式

商務用 Microsoft Store 應用程式是從商務用 Microsoft Store 管理入口網站購買的現代應用程式。然後將它們同步處理至 Microsoft Intune 以進行管理。應用程式可以是線上授權或離線授權。Microsoft Store 直接管理更新，不需要管理員執行其他動作。您也可以使用自訂統一資源識別項 (URI)，避免更新特定的應用程式。如需詳細資訊，請參閱[Enterprise app management-防止應用程式自動更新](#)。使用者也可以停用裝置上所有商務用 Microsoft Store 應用程式的更新。

分類商務用 Microsoft Store 的應用程式

若要分類商務用 Microsoft Store 的應用程式：

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式] > [所有應用程式]。
3. 選取商務用 Microsoft Store 應用程式。然後選取 [屬性 >] [App 資訊 >] 類別。
4. 選取類別。

在 Windows 10 裝置上安裝應用程式

視應用程式類型而定，您可以使用下列兩種方式之一，在 Windows 10 裝置上安裝應用程式：

- **使用者內容**：在使用者內容中部署應用程式時，當使用者登入裝置時，會為該使用者在裝置上安裝受管理的應用程式。請注意，在使用者登入裝置之前，應用程式安裝不會成功。
 - 線上及離線) 皆 (新式 LOB 應用程式和商務用 Microsoft Store 應用程式都可以部署在使用者內容中。應用程式同時支援必要和可用的意向。
 - 以使用者模式或雙重模式為基礎的 Win32 應用程式可以部署在使用者內容中，同時還支援必要和可用的方法。
- **裝置內容**：在裝置內容中部署應用程式時，受管理的應用程式會透過 Intune 直接安裝到裝置。
 - 在裝置內容中只可以部署新式的 LOB 應用程式和離線授權的商務用 Microsoft Store 應用程式。這些

應用程式僅支援必要的目的。

- 以機器模式或雙重模式建立的 Win32 應用程式可以部署在裝置內容中，而且只支援必要的目的。

NOTE

若為以雙重模式應用程式為基礎的 Win32 應用程式，系統管理員必須選擇應用程式是否會做為與該實例關聯之所有工作分派的使用者模式或機器模式應用程式。無法變更每個工作分派的部署內容。

在裝置和 Intune 應用程式類型支援應用程式時，只能在裝置內容中安裝應用程式。在 Windows 10 桌面和 Teams 裝置上都支援安裝裝置內容，例如 Surface Hub。在執行 Windows Holographic for Business 的裝置(例如 Microsoft HoloLens)上不受支援。

您可以在裝置內容中安裝下列應用程式類型，並將這些應用程式指派給裝置群組：

- Win32 應用程式
- 離線授權的商務用 Microsoft Store 應用程式
- LOB 應用程式 (MSI、APPX 及 MSIX)
- 企業版 Microsoft 365 應用程式

Windows LOB 應用程式 (專門的 APPX 和 MSIX) 和商務用 Microsoft Store 應用程式 (您已選取要在裝置內容中安裝的離線應用程式) 必須指派給裝置群組。若使用者內容中已部署其中一個應用程式，安裝就會失敗。系統管理主控台會出現下列狀態和錯誤：

- 狀態：失敗。
- 錯誤：使用者無法以裝置內容安裝為目標。

IMPORTANT

與 Autopilot 預先布建案例搭配使用時，不需要在裝置內容中部署的 LOB 應用程式和商務用 Microsoft Store 應用程式，就可以將設備群組設定成目標。如需詳細資訊，請參閱[Windows Autopilot 預先布建部署](#)。

NOTE

在您儲存具有特定部署的應用程式指派後，您就無法變更該工作分派的內容，但新式應用程式除外。針對新式應用程式，您可以將上下文從使用者內容變更為裝置內容。

如果單一使用者或裝置上的原則有衝突，將會套用下列優先順序：

- 裝置內容原則的優先順序高於使用者內容原則。
- 安裝原則的優先順序高於卸載原則。

如需詳細資訊，請參閱在 [Microsoft Intune 中包含和排除應用程式指派](#)。如需 Intune 中應用程式類型的詳細資訊，請參閱[將應用程式新增至 Microsoft Intune](#)。

後續步驟

- [使用 Microsoft Intune 指派應用程式至群組](#)
- [如何監視應用程式](#)

使用 GCC 高及 DoD 環境上的 Intune 部署應用程式

2022/9/27 •

租使用者系統管理員可以使用 Microsoft Intune 將應用程式發佈至其員工。員工是公司員工，其應用程式的使用者。有許多類型的應用程式可從 GCC 高或 DoD 環境上的 Intune 部署。如果系統管理員需要上傳及發佈 Windows 應用程式，該應用程式適用 DoD GCC 于自訂、由協力廠商廠商建立，或是從[商務用 Microsoft Store](#)下載的離線應用程式，則管理員可以選擇將其散佈為[企業營運應用程式](#)。

NOTE

在商業環境中，租使用者系統管理員可以使用 Intune 將其商務用 Microsoft Store (MSFB) 同步處理，但是針對 GCC 高和 DoD 環境，此服務無法使用。在此情況下，系統管理員必須直接上傳至 Intune，部署應用程式。若要取得所需的應用程式的 offline 版本，必須使用實際的商務用帳戶登入 MSFB，以下載套件，這是目前只有 GCC 高和 DOD 環境的工作情形。

使用 Intune 新增商務營運應用程式

若要使用 Intune 為 GCC 高或 DoD 環境的企業營運應用程式新增，您可以遵循[Windows 的 LOB 應用程式](#)指示。您可以選擇先從商務用 Microsoft Store 部署公司入口網站。如果您選擇使用公司入口網站，您可以手動安裝及部署公司入口網站。如需詳細資訊，請參閱 [how to configure the Microsoft Intune 公司入口網站應用程式](#)。

使用 Intune 從商務用店發佈離線應用程式

如果您需要從商務用 Microsoft Store [下載離線授權的應用程式](#)，請遵循下列步驟下載應用程式：

1. 登入商務用 [店](#)。
2. 選取 [管理 > 設定]。
3. 在 [購物經驗] 底下，設定 [顯示離線應用程式]。

當您購買應用程式時，如果有離線版本可供使用，您可以選擇將授權類型變更為離線。在取得應用程式之後，您可以在 [商務用店](#) 中選擇 [管理 > 產品 & 服務]，以進行管理。此外，您也可以下載應用程式及其相依性。然後，您可以使用 Intune 來部署此下載的應用程式 (及其相依性) 給使用者。

同步處理 Intune 至商務用店

在商業 (非政府) 環境中，系統管理員可以將 Intune 同步處理至商務用 Microsoft Store。這不是政府環境中的可用功能。如需商業環境和政府環境 Intune 中 Intune 之間差異的詳細資訊，請參閱[Enterprise Mobility + Security 美國政府服務說明](#)。

若要將 Intune 同步處理至您的商務用商店帳戶，請參閱 [how to manage the the the the 商務用 Microsoft Store with Microsoft Intune 購買的應用程式](#)。

合規性

在評估適當使用服務時，請查看應用程式的隱私權和符合性聲明，並與組織的相容性、安全性和隱私權需求進行比較。

後續步驟

若要深入瞭解部署和指派應用程式的相關資訊, 請參閱[使用 Microsoft Intune 指派應用程式給群組](#)。

2022/9/27 •

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式] > [所有應用程式]。
3. 在應用程式清單中，選取要監視的應用程式。接著，您會看到應用程式窗格，其中包含裝置狀態和使用者狀態的概觀。

從 Windows 公司入口網站或公司入口網站網站的 [已] 頁面，終端使用者可以檢視裝置指派必要應用程式的安裝狀態和詳細資料。除了使用者指派必要應用程式的安裝狀態和詳細資料之外，還會提供這項功能。

XXXXXXXXXX	“
Publisher	應用程式的發行者。
■	應用程式作業系統 (Windows、iOS/iPadOS、Android 等)。
■	建立此修訂的日期和時間。■:■ IT ■■■■■■, ■■■, ■■■■ ■■■
■	是否已指派應用程式 (■ 或 ■)。

圖例	說明
Installed	已安裝的應用程式數目。
■	未安裝的應用程式數目。
■	失敗的安裝數目。
■	正在安裝的應用程式數目。

欄位名稱	說明
裝置安裝狀態	狀態不適用的應用程式數目。

NOTE

請注意, Android LOB 應用程式 (.APK) 部署為 [Android], 只會報告已註冊裝置的應用程式安裝狀態。未在 Intune 中註冊的裝置無法使用應用程式安裝狀態。

裝置安裝狀態

當您在功能表的 [監視] 區段中選取 [裝置安裝狀態] 時, 會顯示裝置狀態清單。詳細資料表包含下列資料行:

欄位名稱	說明
裝置名稱	允許命名裝置之平臺上的裝置名稱。在其他平臺上, Intune從其他屬性建立名稱。此屬性不適用於任何其他裝置。
使用者名稱	使用者的名稱。
作業系統	裝置的作業系統 (Windows、iOS/iPadOS、Android 等)。
應用程式版本	應用程式的版本號碼。針對企業營運 (LOB) 應用程式和商務用 Microsoft Store應用程式, 會顯示應用程式的完整版本號碼。完整版本號碼會識別應用程式的特定版本。此數位會顯示為 版本 (組建)。例如, 2.2 (2.2.17560800)。針對標準市集應用程式, 不會顯示任何版本。
安裝狀態	應用程式的狀態。
安裝日期	狀態的詳細資料。
上次同步日期	裝置上次與Intune同步的日期。

NOTE

即使應用程式的目標為裝置內容和裝置群組, 一律會報告使用者名稱。您可以參考對應的 [API 呼叫](#)。此外, 系統內容可能會顯示為「沒有使用者」。

使用者安裝狀態

當您在功能表的 [監視] 區段中選取 [使用者安裝狀態] 時, 會顯示使用者狀態清單。詳細資料表包含下列資料行:

欄位名稱	說明
Name	Azure Active Directory 中的使用者名稱。
唯一名稱	使用者的唯一名稱。
安裝數目	使用者安裝的應用程式數目。
失敗安裝數目	使用者失敗的應用程式安裝數目。

■	使用者未安裝的應用程式數目。

後續步驟

- 若要深入瞭解如何使用Intune資料，請參閱[使用Intune Data Warehouse](#)。
- 若要瞭解應用程式設定原則，請參閱[適用於Intune的應用程式設定原則](#)。

Intune探索到的應用程式

2022/9/27 •

Intune探索到的 **應用程式** 是租使用者中已註冊Intune裝置上偵測到的應用程式清單。它可作為租使用者的軟體清查。**探索到的應用程式** 是與 **應用程式安裝** 報告不同的報表。針對個人裝置，Intune永遠不會收集 Unmanaged 應用程式的相關資訊。在公司裝置上，不論其是否為受控應用程式，系統會針對此報表收集任何應用程式。以下是對應預期行為的資料表。一般而言，報表會從註冊開始每隔 7 天重新整理一次，（整個租使用者）每週重新整理一次。探索到的應用程式報告此重新整理週期的唯一例外是透過 Win32 **應用程式** 的Intune管理延伸模組收集的應用程式資訊，每 24 小時收集一次。

使用 Intune 監視探索到的應用程式

Intune提供租使用者中已註冊Intune裝置上偵測到的應用程式匯總清單。

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 > 監視器 > 探索到的應用程式]。

NOTE

您可以 ■ [探索到的應用程式] 窗格中選取 [匯出]，將探索到的 ■ 清單匯出至.csv檔案。

針對探索到的 Win32 應用程式，目前沒有匯總計數。這種類型的資料只能以每個裝置為基礎來檢視。

Intune也提供租使用者中個別裝置探索到的應用程式清單。

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 裝置的裝置]。
3. 選取裝置。
4. 若要檢視此裝置偵測到的應用程式，請在 [監視] 區段中選取 [探索到的 應用程式]。

探索到的應用程式詳細資料

下列清單提供應用程式平臺類型、針對個人裝置監視的應用程式、針對公司擁有的裝置監視的應用程式，以及重新整理週期。如需Intune所支援之應用程式類型的詳細資訊，請參閱[Microsoft Intune 中的應用程式類型](#)。

OS	裝置類型	裝置上安裝的應用程式	重新整理週期
Windows 10/11 (Win32 Apps) 注意: 裝置上需要 Intune管理延伸模組	不適用	裝置上已安裝 MSI 的應用程式	從裝置註冊開始每隔 24 小時
Windows 10/11 (Modern Apps)	僅限 Managed 新式應用程式	裝置上安裝的所有新式應用程式	從裝置註冊開始每隔 7 天
Windows 8.1	僅限 Managed 應用程式	僅限 Managed 應用程式	從裝置註冊開始每隔 7 天
Windows RT	僅限 Managed 應用程式	僅限 Managed 應用程式	從裝置註冊開始每隔 7 天
iOS/iPadOS	僅限 Managed 應用程式	裝置上安裝的所有應用程式	從裝置註冊開始每隔 7 天

OS	Application Type	Applications	Frequency
macOS	僅限 Managed 應用程式	裝置上安裝的所有應用程式	從裝置註冊開始每隔 7 天
Android	僅限 Managed 應用程式	裝置上安裝的所有應用程式	從裝置註冊開始每隔 7 天
Android 企業版	僅限 Managed 應用程式	僅安裝在 Android Enterprise 工作設定檔裝置上的應用程式	從裝置註冊開始每隔 7 天

NOTE

- Windows 10/11 共同管理的裝置，如 Configuration Manager 中的 [用戶端應用程式](#) 工作負載所示，目前不會根據上述排程，透過 Intune 管理延伸模組 (IME) 收集應用程式清查。若要減輕此問題，應將 Configuration Manager 中的 [用戶端應用程式](#) 工作負載切換為 Intune，才能在裝置上安裝 IME，(Win32 清查和 PowerShell 部署) 需要 IME。請注意，此行為的任何變更或更新都會在 [開發](#) 和/或 [新功能](#) 中公告。
- 在 2019 年 11 月之前註冊的個人擁有 macOS 裝置可能會繼續顯示裝置上安裝的所有應用程式，直到裝置再次註冊為止。
- Android Enterprise 完全受控、專用和 Corporate-Owned 工作設定檔裝置不會顯示探索到的應用程式。
- 對於使用 Mobile Threat Defense 合作夥伴與 Intune 的客戶，[應用程式同步資料](#) 會根據裝置簽入的間隔傳送給 Mobile Threat Defense 合作夥伴，且不應與探索到的應用程式報告的重新整理間隔混淆。

探索到的應用程式數目可能不符合應用程式安裝狀態計數。不一致的可能性包括：

- 已安裝受控應用程式的目標變更可能會導致狀態窗格中的安裝計數遞減，但在偵測到的應用程式中仍會回報。
- 以租使用者中相同應用程式的多個實例為目標，會導致因使用者或裝置可能重迭而導致不同的計數。應用程式的每個實例都會計算重迭的使用者，但探索到的應用程式會有重複的計數。
- 探索到的應用程式和應用程式狀態會以不同的時間間隔收集，這可能會導致應用程式計數不一致。

後續步驟

- [Microsoft Intune 中的應用程式類型](#)
- [使用 Microsoft Intune 監視應用程式資訊和指派](#)

Microsoft Intune 的應用程式組態原則

2022/9/27 •

應用程式設定原則可讓您將組態設定指派給在使用者執行應用程式之前指派給使用者的原則，協助您消除應用程式設定問題。然後，當使用者裝置上設定應用程式，且使用者不需要採取動作時，就會自動提供這些設定。每個應用程式的組態設定都是唯一的。

您可以建立並使用應用程式設定原則，為iOS/iPadOS 或Android應用程式提供組態設定。這些組態設定可讓您使用應用程式組態和管理來自訂應用程式。當應用程式檢查這些設定時，通常會在第一次執行應用程式時，使用組態原則設定。

例如，應用程式組態設定可能需要您指定下列任何詳細資料：

- 自訂埠號碼
- 語言設定
- 安全性設定
- 商標設定，例如公司標誌

如果終端使用者改為輸入這些設定，可能會不正確地執行此動作。應用程式設定原則可協助在企業之間提供一致性，並減少使用者嘗試自行設定設定的技術服務人員呼叫。使用應用程式設定原則，可以更輕鬆且快速地採用新的應用程式。

可用的組態參數和組態參數的實作是由應用程式的開發人員決定。應檢閱應用程式廠商的檔，以查看可用的設定，以及設定如何影響應用程式的行為。對於某些應用程式，Intune會填入可用的組態設定。

NOTE

在 Managed Google Play 商店中，支援設定的應用程式會標示如下：



使用受控裝置作為Android裝置的註冊類型時，您只會看到來自受控Google Play存放區的應用程式，而非Google Play存放區。

您可以使用 [包含和排除指派](#) 的組合，將應用程式設定原則指派給一組使用者和裝置。在新增或更新應用程式設定原則的過程中，您可以設定應用程式設定原則的指派。當您設定原則的指派時，可以選擇包含和排除套用原則的使用者 [群組](#)。當您選擇包含一或多個群組時，可以選擇選取要包含或選取內建群組的特定群組。內建群組包括 [\[所有使用者\]](#)、[\[所有裝置\]](#) 和 [\[所有使用者 + 所有裝置\]](#)。

應用程式設定原則工作負載會提供已為租使用者建立的應用程式設定原則清單。此清單提供詳細資料，例如名稱、平臺、已更新、註冊類型和範圍標籤。如需特定應用程式設定原則的其他詳細資料，請選取原則。在 [\[原則概觀\]](#) 窗格中，您可以查看特定詳細資料，例如根據裝置和使用者的原則狀態，以及是否已指派原則。

支援應用程式設定的應用程式

應用程式設定可以透過已註冊裝置上的行動裝置管理 (MDM) OS 通道 (iOS的受控[應用程式組態](#)通道, 或 Android) Enterprise通道[中的Android](#), 或透過行動應用程式管理 (MAM) 通道傳遞。

Intune將這些不同的應用程式設定原則通道表示為：

- **受控裝置**- 裝置由Intune作為統一端點管理提供者來管理。應用程式必須釘選到 iOS/iPadOS 上的管理設定檔, 或透過Android裝置上的受控Google Play部署。此外, 應用程式支援所需的應用程式設定。
- **受控應用程式**- 已整合 Intune App SDK 或已使用Intune包裝工具組裝, 並支援應用程式) (應用程式保護原則的應用程式。在此設定中, 裝置的註冊狀態或應用程式傳遞至裝置的方式都無關緊要。應用程式支援所需的應用程式設定。

* Device enrollment type ⓘ



應用程式可能會根據使用者喜好設定, 以不同的方式處理應用程式設定原則設定。例如, 使用iOS和Android的Outlook, 焦點收件匣應用程式組態設定會遵守使用者設定, 讓使用者能夠覆寫系統管理員意圖。其他設定可讓您控制使用者是否可以或無法根據系統管理員意圖來變更設定。

NOTE

Intune需要 Android 8.x 或更新版本才能進行裝置註冊案例, 以及透過受控裝置應用程式設定原則傳遞的應用程式設定。此需求不適用於 [Microsoft Teams Android 裝置](#), 因為這些裝置將繼續受到支援。

針對Intune應用程式保護原則和透過 Managed 應用程式應用程式設定原則傳遞的應用程式設定, Intune需要 Android 9.0 或更新版本。

受控裝置

選取 [受管理的裝置] 作為 [裝置註冊類型], 特別是指Intune在已註冊裝置上部署的應用程式, 因此由Intune作為註冊提供者來管理。

若要支援在已註冊裝置上透過Intune部署之應用程式的應用程式設定, 必須撰寫應用程式以支援使用作業系統所定義的應用程式設定。如需其支援透過 MDM OS 通道傳遞的應用程式設定金鑰詳細資訊, 請洽詢您的應用程式廠商。使用 MDM OS 通道的應用程式設定傳遞通常有四種案例：

- 只允許公司或學校帳戶
- 帳戶設定組態設定
- 一般應用程式組態設定
- S/MIME 組態設定

受管理應用程式

選取 [受控應用程式] 作為 [裝置註冊類型], 特別是指在裝置上使用Intune應用程式保護原則設定的應用程式, 而不論註冊狀態為何。

若要透過 MAM 通道支援應用程式設定, 應用程式必須與[Intune App SDK](#)整合。企業營運應用程式可以整合 Intune App SDK 或使用[Intune App Wrapping Tool](#)。如需 Intune App SDK 與Intune App Wrapping Tool之間的比較, 請參閱[準備應用程式保護原則的企業營運應用程式](#)。

透過 MAM 通道傳遞應用程式設定時, 不需要註冊裝置, 也不需要透過統一端點管理解決方案來管理或傳遞應用

程式。使用 MAM 通道進行應用程式設定傳遞的案例有三種：

- 一般應用程式組態設定
- S/MIME 組態設定
- 進階 APP 資料保護設定，可擴充應用程式保護原則所提供的功能

NOTE

Intune受控應用程式會與Intune應用程式保護原則一起部署時，Intune 應用程式組態原則狀態的間隔為 30 分鐘來簽入。如果未將Intune應用程式保護原則指派給使用者，則Intune 應用程式組態原則簽入間隔會設定為 720 分鐘。

如需哪些應用程式透過 MAM 通道支援應用程式設定的相關資訊，請參閱[Microsoft Intune受保護的應用程式](#)。

Android Enterprise應用程式設定原則

針對Android Enterprise應用程式設定原則，您可以在建立應用程式組態設定檔之前選取裝置註冊類型。您可以考慮以註冊類型為基礎的憑證設定檔。

註冊類型可以是下列其中一種：

- **所有配置檔案類型**：如果已建立新的設定檔，且已針對裝置註冊類型選取 [所有配置檔案類型]，您將無法將憑證設定檔與應用程式設定原則產生關聯。此選項支援使用者名稱和密碼驗證。如果您使用憑證式驗證，請勿使用此選項。
- **僅限完全受控、專用和Corporate-Owned工作設定檔**：如果已建立新的設定檔，且只選取 [完全受控]、[專用] 和 [Corporate-Owned工作配置 檔]，則可以使用 [裝置 > 組態 設定檔] 底下建立的 [完全受控]、[專用] 和 [Corporate-Owned工作設定檔] 憑證原則。此選項支援憑證式驗證，以及使用者名稱和密碼驗證。完全受控 與 COBO) (Android Enterprise完全受控裝置有關。專用 與 COSU) (Android Enterprise專用裝置有關。公司擁有的工作設定檔 與ANDROID ENTERPRISE公司擁有的工作設定檔 () 相關。
- **僅限個人擁有的工作設定檔**：如果建立新的設定檔，並選取 [僅限個人擁有的工作設定檔]，則可以使用在 [裝置 > 組態 設定檔] 下建立的工作設定檔憑證原則。此選項支援憑證式驗證，以及使用者名稱和密碼驗證。

NOTE

如果您將 Gmail 或 Nine 組態設定檔部署到不涉及使用者的Android Enterprise專用裝置工作設定檔，則會失敗，因為Intune無法解析使用者。

IMPORTANT

此功能發行前建立的現有原則 (2020 年 4 月版本 - 2004 年) 若沒有任何與該原則相關聯的憑證設定檔，則預設為裝置註冊類型的 。此外，在發行此功能之前建立且具有相關聯憑證設定檔的現有原則，預設為僅限工作設定檔。

現有原則將不會補救或發行新的憑證。

驗證套用的應用程式設定原則

您可以使用下列三種方法來驗證應用程式設定原則：

1. 在裝置上以可見的方式驗證應用程式設定原則。確認目標應用程式呈現應用程式設定原則中套用的行為。
2. 透過診斷記錄進行驗證 (請參閱下方 [的診斷記錄](#) 一節)。
3. 在Microsoft 端點管理員系統管理中心確認。在 [Microsoft 端點管理員系統管理中心](#)，選取 [應用程式 >] [所有應用程式 > [選取相關的應用程式]]。然後，在 [監視] 區段下，選取 [裝置安裝狀態] 或 [使用者安

裝狀態]：

MDM-Outlook ios - Device install status

Search (Ctrl+/) Export Filter

Filter items...

DEVICE NAME	USER NAME	STATUS
Steve's iPad	None	Pending
Steve's iPhone	AdeleV@M365x935807.OnMicrosoft.com	Succeeded

MDM-Outlook ios - User install status

Search (Ctrl+/) Export Filter

Filter items...

USER NAME	DEVICE COUNT	STATUS
AdeleV@M365x935807.OnMicrosoft.com	2	Succeeded

此外，在 [Microsoft 端點管理員 系統管理中心](#) 內，選取 [裝置 > 所有裝置 >] 選取裝置 > 應用程式設定。應用程式組態** 窗格會顯示所有指派的原則及其狀態：

Home > Microsoft Intune > Devices - All devices > Steve's iPad - App configuration

Steve's iPad - App configuration

Search (Ctrl+/) Export

Filter by name

POLICY	USER PRINCIPAL NAME	STATE
MDM-Edge	AdeleV@M365x935807.OnMicrosoft.com	Succeeded
MDM-Outlook ios	AdeleV@M365x935807.OnMicrosoft.com	Succeeded
MDM-Managed Browser	AdeleV@M365x935807.OnMicrosoft.com	Succeeded

診斷記錄

unmanaged 裝置上的 iOS/iPadOS 設定

您可以使用Intune **診斷記錄** 來驗證iOS/iPadOS 設定，以取得透過 Managed 應用程式設定原則部署的設定。除了下列步驟之外，您還可以使用 Microsoft Edge 存取受控應用程式記錄檔。如需詳細資訊，請參閱[使用 Edge 來 iOS和Android存取受控應用程式記錄](#)。

1. 如果尚未安裝在裝置上，請從 App Store 下載並安裝Microsoft Edge。如需詳細資訊，請參閱[Microsoft Intune受保護的應用程式](#)。
2. 啟動 Microsoft Edge，然後在 [位址]方塊中輸入 about:intunehelp。
3. 按一下 [入門]。
4. 按一下 [共用記錄]。
5. 使用您選擇的郵件應用程式將記錄傳送給您自己，以便在您的電腦上檢視。

6. 檢閱文字檔檢視器中的 IntuneMAMDiagnostics.txt 。

7. ApplicationConfiguration 搜尋。結果如下所示：

```
{
  (
    {
      Name = "com.microsoft.intune.mam.managedbrowser.BlockListURLs";
      Value = "https://www.aol.com";
    },
    {
      Name = "com.microsoft.intune.mam.managedbrowser.bookmarks";
      Value = "Outlook Web|https://outlook.office.com|Bing|https://www.bing.com";
    }
  );
},
{
  ApplicationConfiguration =
  (
    {
      Name = IntuneMAMUPN;
      Value =
"CMARScrubbedM:13c45c42712a47a1739577e5c92b5bc86c3b44fd9a27aeec3f32857f69ddef79cbb988a92f8241af6df8b3
ced7d5ce06e2d23c33639ddc2ca8ad8d9947385f8a";
    },
    {
      Name = "com.microsoft.outlook.Mail.BlockExternalImagesEnabled";
      Value = true;
    }
  );
}
```

您的應用程式設定詳細資料應該符合為租使用者設定的應用程式設定原則。

Targeted App Config - Configuration

Search (Ctrl+/) Save Discard

General Assignments Targeted apps Configuration Scope (Tags)

Intune SDK-enabled apps support configurations in key-value pairs. Consult the documentation for each app to learn more about which key-value configurations are supported.

Intune supports string values and token replacement values.

[Learn more about which tokens Intune supports](#)

NAME	VALUE
com.microsoft.intune.mam.managedbrowser.BlockListU...	https://www.aol.com
com.microsoft.intune.mam.managedbrowser.bookmarks	Outlook Web https://outlook.office.com Bing https://w...

受控裝置上的 iOS/iPadOS 設定

您可以使用受控裝置上的Intune診斷記錄來驗證受控應用程式設定的iOS/iPadOS 設定。

1. 如果尚未安裝在裝置上，請從 App Store 下載並安裝Microsoft Edge。如需詳細資訊，請參閱[Microsoft Intune受保護的應用程式](#)。
2. 啟動 Microsoft Edge，然後在 [位址]方塊中輸入 about:intunehelp。
3. 按一下 [入門]。
4. 按一下 [共用記錄]。
5. 使用您選擇的郵件應用程式將記錄傳送給您自己，以便在您的電腦上檢視。
6. 檢閱文字檔檢視器中的 IntuneMAMDiagnostics.txt 。
7. AppConfig 搜尋。您的結果應該符合為租使用者設定的應用程式設定原則。

受管理裝置上的Android設定

您可以使用受控裝置上的 **Intune診斷記錄** 來驗證受控應用程式設定的Android組態。

若要從Android裝置收集記錄，您或終端使用者必須透過 USB 連線 (或裝置) 上的 **檔案總管** 對等專案，從裝置下載記錄。步驟如下：

1. 使用 USB 纜線將Android裝置連線到您的電腦。

2. 在電腦上，尋找具有裝置名稱的目錄。在該目錄中，尋找

`Android Device\Phone\Android\data\com.microsoft.windowsintune.companyportal`。

3. 在 資料夾中 `com.microsoft.windowsintune.companyportal`，開啟 [檔案] 資料夾，然後開啟 `QMADMLog_0`。

4. `AppConfigHelper` 搜尋 以尋找應用程式設定相關的訊息。結果看起來會類似下列資料區塊：

```
2019-06-17T20:09:29.1970000 INFO AppConfigHelper 10888 02256 Returning app config JSON
[{"ApplicationConfiguration":
[{"Name": "com.microsoft.intune.mam.managedbrowser.BlockListURLs", "Value": "https://www.aol.com"},
{"Name": "com.microsoft.intune.mam.managedbrowser.bookmarks", "Value": "Outlook
Web|https://outlook.office.com|Bing|https://www.bing.com"},
{"Name": "com.microsoft.intune.mam.managedbrowser.homepage", "Value": "https://www.arstechnica.com"}]},
{"ApplicationConfiguration": [{"Name": "IntuneMAMUPN", "Value": "AdeleV@M365x935807.OnMicrosoft.com"},
{"Name": "com.microsoft.outlook.Mail.NotificationsEnabled", "Value": "false"},
{"Name": "com.microsoft.outlook.Mail.NotificationsEnabled.UserChangeAllowed", "Value": "false"}]}] for
user User-875363642
```

圖形 API支援應用程式設定

您可以使用圖形 API來完成應用程式設定工作。如需詳細資訊，請參閱[圖形 API參考 MAM 目標設定](#)。如需Intune和Graph的詳細資訊，請參閱在[Microsoft Graph 中使用Intune](#)。

疑難排解

使用記錄來顯示組態參數

當記錄顯示已確認要套用但似乎無法運作的組態參數時，應用程式開發人員的組態實作可能會發生問題。先連絡該應用程式開發人員，或檢查其知識庫，可能會為您省下 Microsoft 的支援電話。如果這是在應用程式內處理設定的方式問題，則必須在該應用程式的未來更新版本中加以解決。

後續步驟

受控裝置

- 瞭解如何將應用程式設定與您的iOS/iPadOS 裝置搭配使用。請參閱[新增受控iOS/iPadOS 裝置的應用程式設定原則](#)。
- 瞭解如何搭配您的Android裝置使用應用程式設定。請參閱[新增受控Android裝置的應用程式設定原則](#)。

受管理應用程式

- 瞭解如何搭配受控應用程式使用應用程式設定。請參閱 [為未註冊裝置的受控應用程式新增應用程式設定原則](#)。

新增受管理 iOS/iPadOS 裝置的應用程式設定原則

2022/9/27 •

使用 Microsoft Intune 中的應用程式設定原則，為 iOS/iPadOS 應用程式提供自訂群組態設定。這些組態設定可讓您根據應用程式供應商方向自訂應用程式。您必須從應用程式的供應商取得這些組態設定（金鑰和值）。若要設定應用程式，您可以將設定指定為索引鍵和值，或指定為包含索引鍵和值的 XML。

身為 Microsoft Intune 系統管理員，您可以控制要將哪些使用者帳戶新增至受管理裝置上的 Microsoft Office 應用程式。您可以限制只能存取允許的組織使用者帳戶，並封鎖已註冊裝置上的個人帳戶。支援的應用程式會處理應用程式設定，並移除和封鎖未核准的帳戶。當應用程式檢查組態原則設定時，通常會在第一次執行時使用。

新增應用程式設定原則之後，您可以設定應用程式設定原則的指派。當您設定原則的指派時，可以選擇包含和排除套用原則的使用者群組。當您選擇包含一或多個群組時，可以選擇選取要包含或選取內建群組的特定群組。內建群組包括 [所有使用者]、[所有裝置] 和 [所有使用者 + 所有裝置]。

NOTE

Intune 提供主控台中預先建立 [] 和 [] 群組，並提供內建優化以方便您使用。強烈建議您使用這些群組以所有使用者和所有裝置為目標，而不是您自己建立的任何「所有使用者」或「所有裝置」群組。

為應用程式設定原則選取包含的群組之後，您也可以選擇要排除的特定群組。如需詳細資訊，請參閱 [在 Microsoft Intune 中包含和排除應用程式指派](#)。

TIP

此原則類型目前僅適用於執行 iOS/iPadOS 8.0 和更新版本的裝置。它支援下列應用程式安裝類型：

- Managed iOS/iPadOS
- iOS

如需應用程式安裝類型的詳細資訊，請參閱 [如何將應用程式新增至 Microsoft Intune](#)。如需將應用程式組態併入受控裝置 .ipa 應用程式套件的詳細資訊，請參閱 [iOS 開發人員檔](#) 中的受控應用程式組態。

建立應用程式設定原則

- 登入 [Microsoft 端點管理員系統管理中心](#)。
- 選擇 [應用程式 >] 設定原則 > [新增 > 受控裝置]。請注意，您可以在受控裝置和受控應用程式之間進行選擇。如需詳細資訊，請參閱 [支援應用程式設定的應用程式](#)。
- 在 [基本] 頁面上，設定下列詳細資料：
 - 名稱 - 出現在 Microsoft 端點管理員系統管理中心的設定檔名稱。
 - 描述 - 出現在 Microsoft 端點管理員系統管理中心的設定檔描述。
 - 裝置註冊類型 - 此設定設為受控裝置。
- 選取 [iOS/iPadOS] 作為 [平臺]。
- 按一下 [目標應用程式] 旁的 [選取應用程式]。[相關聯的應用程式] 窗格隨即顯示。
- 在 [目標應用程式] 窗格中，選擇要與設定原則相關聯的受控應用程式，然後按一下 [確定]。
- 按一下 [下一步] 以顯示 [設定] 頁面。

8. 在下拉式方塊中，選取 [組態設定] 格式。選取下列其中一個方法來新增組態資訊：

- 使用設定設計工具
- 輸入 XML 資料

如需使用設定設計工具的詳細資訊，請 [參閱使用設定設計工具](#)。如需輸入 XML 資料的詳細資訊，請 [參閱輸入 XML 資料](#)。

9. 按 [下一步] 以顯示 [指派] 頁面。

10. 在 [指派給] 旁的下拉式方塊中，選取 [選取的群組]、[所有使用者]、[所有裝置] 或 [所有使用者和所有開發人員] 來指派應用程式設定原則。

The screenshot shows the 'Assignments' step of a configuration wizard. At the top, there are four tabs: 'Basics' (checked), 'Settings' (checked), '3 Assignments' (active), and '4 Review + create'. Below the tabs, the 'Included groups' section has an 'Assign to' dropdown menu currently showing 'Selected groups'. Underneath this is a list titled 'Selected groups' which is currently empty, displaying 'No groups selected'. A link '+ Select groups to include' is provided below the list. The 'Excluded groups' section also has a list titled 'Selected groups' which is empty, displaying 'No groups selected', with a link '+ Select groups to exclude' below it. A light blue informational box with an 'i' icon contains the text: 'When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.' At the bottom of the form, there are two buttons: 'Previous' and 'Next'.

11. 在下拉式方塊中選取 [所有使用者]。

Create app configuration policy

✓ Basics ✓ Settings **3 Assignments** 4 Review + create

Included groups

Assign to

All users

Excluded groups

 When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more.](#)

Selected groups

No groups selected

[+ Select groups to exclude](#)

Previous

Next

12. 按一下 [選取要排除的群組] 以顯示相關窗格。

Select groups to exclude

Azure AD Groups

Select ⓘ

Search by name or email address

✓

AD

ADSyncAdmins

AD

ADSyncBrowse

AD

ADSyncOperators

Selected members:

No members selected

Select

13. 選擇您想要排除的群組，然後按一下 [選取]。

NOTE

新增群組時，如果指定的指派類型已包含任何其他群組，則會預先選取該群組，而且對於其他 include 指派類型則無法變更。因此，該群組已使用，不能當做排除的群組使用。

14. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。

15. 按一下 [建立] 將應用程式設定原則新增至Intune。

使用設定設計工具

Microsoft Intune提供應用程式唯一的組態設定。您可以針對已註冊或未在 Microsoft Intune 中註冊之裝置上的應用程式使用設定設計工具。設計工具可讓您設定特定的組態索引鍵和值，以協助您建立基礎 XML。您也必須為每個值指定資料類型。這些設定會在安裝應用程式時自動提供給應用程式。

新增設定

- 針對組態中的每個索引鍵和值，設定：
 - 組態金鑰** - 唯一識別特定設定組態的區分大小寫金鑰。
 - 實數值型別** - 組態值的資料類型。類型包括 Integer、Real、String 或 Boolean。
 - 組態值** - 組態的值。
- 選擇 [確定] 以設定組態設定。

刪除設定

- 選擇設定旁的省略號 (...)。
- 選取 [刪除]。

和 {{}} 字元僅供權杖類型使用，不得用於其他用途。

只允許應用程式中已設定的組織帳戶

身為 Microsoft Intune 系統管理員，您可以控制要將哪些公司或學校帳戶新增至受管理裝置上的 Microsoft 應用程式。您可以限制只能存取允許的組織使用者帳戶，並在已註冊的裝置上支援，封鎖應用程式 (內的個人帳戶。針對 iOS/iPadOS 裝置，請在受控裝置應用程式設定原則中使用下列機碼/值組：

機碼	值
IntuneMAMAllowedAccountsOnly	■: 唯一允許的帳戶是 IntuneMAMUPN 金鑰所定義的受管理使用者帳戶。 ■ 用 (或任何與 Enabled 不區分大小寫相符的值) : 允許任何帳戶。
IntuneMAMUPN	- 允許登入應用程式的帳戶 UPN。 - 針對 Intune 註冊的 {{userprincipalname}} 裝置，可以使用權杖來代表已註冊的使用者帳戶。

NOTE

下列應用程式會處理上述應用程式設定，且只允許組織帳戶：

- 適用於 iOS (44.8.7 和更新版本的 Edge)
- Office、Word、Excel、PowerPoint for iOS (2.41 和更新版本)
- 適用於 iOS (10.34 和更新版本的 OneDrive)
- 適用於 iOS (2.41 和更新版本的 OneNote)
- iOS 版 Outlook (2.99.0 和更新版本)
- 適用於 iOS (2.0.15 和更新版本的 Teams)

需要在應用程式中設定組織帳戶

在已註冊的裝置上，組織可以要求公司或學校帳戶已登入受控 Microsoft 應用程式，才能接收來自其他受控應用程式的組織資料。例如，假設使用者的附件包含在原生 iOS 郵件用戶端的 Managed 電子郵件設定檔內的電子郵件訊息中。如果使用者嘗試將附件傳輸至在裝置上管理且已套用這些金鑰的 Microsoft 應用程式，例如 Office，則此設定會將傳輸的附件視為組織資料，要求公司或學校帳戶必須登入並強制執行應用程式保護原則設定。

針對 iOS/iPadOS 裝置，請在每個 Microsoft 應用程式的受控裝置應用程式設定原則中使用下列機碼/值組：

IntuneMAMRequireAccounts	IntuneMAMUPN
IntuneMAMRequireAccounts	- 已啟用: 應用程式需要使用者登入 IntuneMAMUPN 金鑰所定義的受控使用者帳戶, 才能接收組織資料。 - 停用 (或任何與 Enabled 不區分大小寫相符的值) : 不需要帳戶登入
IntuneMAMUPN	- 允許登入應用程式的帳戶 UPN。 - 針對Intune註冊的 <code>{{userprincipalname}}</code> 裝置, 可以使用權杖來代表已註冊的使用者帳戶。

NOTE

應用程式必須Intune適用於 iOS 12.3.3 版或更新版本的 APP SDK, 並在要求登入公司或學校帳戶時, 以[Intune應用程式保護](#)原則作為目標。在應用程式保護原則中, [接收來自其他應用程式的資料] 必須設定為 [具有傳入組織資料的所有應用程式]。

目前, 只有當目標應用程式有傳入組織資料時, 才需要應用程式登入。

輸入 XML 資料

您可以輸入或貼上 XML 屬性清單, 其中包含在 Intune 中註冊之裝置的應用程式組態設定。XML 屬性清單的格式會根據您要設定的應用程式而有所不同。如需要使用之確切格式的詳細資訊, 請連絡應用程式的供應商。

Intune驗證 XML 格式。不過, Intune不會檢查 PList (XML 屬性清單) 是否適用於目標應用程式。

若要深入瞭解 XML 屬性清單:

- 請參閱 iOS 開發人員程式庫中的 [瞭解 XML 屬性清單](#)。

應用程式組態 XML 檔案的範例格式

當您建立應用程式組態檔時, 可以使用此格式指定下列一或多個值:

```
<dict>
  <key>userprincipalname</key>
  <string>{{userprincipalname}}</string>
  <key>mail</key>
  <string>{{mail}}</string>
  <key>partialupn</key>
  <string>{{partialupn}}</string>
  <key>accountid</key>
  <string>{{accountid}}</string>
  <key>deviceid</key>
  <string>{{deviceid}}</string>
  <key>userid</key>
  <string>{{userid}}</string>
  <key>username</key>
  <string>{{username}}</string>
  <key>serialnumber</key>
  <string>{{serialnumber}}</string>
  <key>serialnumberlast4digits</key>
  <string>{{serialnumberlast4digits}}</string>
  <key>udidlast4digits</key>
  <string>{{udidlast4digits}}</string>
  <key>aaddeviceid</key>
  <string>{{aaddeviceid}}</string>
  <key>IsSupervised</key>
  <string>{{IsSupervised}}</string>
</dict>
```

支援的 XML PList 資料類型

Intune在屬性清單中支援下列資料類型：

- <整數>
- <真正>
- <字串>
- <陣 列>
- <dict>
- <true /> 或 < false />

屬性清單中使用的權杖

此外，Intune在屬性清單中支援下列權杖類型：

- {{userprincipalname}} —例如 John @ contoso.com
- {{mail}} —例如 John @ contoso.com
- {{partialupn}} -例如 John
- {{accountid}} —例如 fc0dc142-71d8-4b12-bbea-bae2a8514c81
- {{deviceid}} —例如 b9841cd9-9843-405f-be28-b2265c59ef97
- {{userid}} —例如 3ec2c00f-b125-4519-acf0-302ac3761822
- {{username}} —例如 John Doe
- {{serialnumber}} -例如，iOS/iPadOS 裝置的 F4KN99ZUG5V2 ()
- {{serialnumberlast4digits}} -例如，適用於 iOS/iPadOS 裝置的 G5V2 ()
- {{aaddeviceid}} —例如 ab0dc123-45d6-7e89-aabb-cde0a1234b56
- {{受監督}} —例如，iOS/iPadOS 裝置的 True ()

設定公司入口網站應用程式以支援使用自動裝置註冊註冊的 iOS 和 iPadOS 裝置

根據預設，Apple 的自動裝置註冊與公司入口網站應用程式的應用程式市集版本不相容。不過，即使使用者已使

用下列步驟從App Store下載公司入口網站，您也可以將公司入口網站應用程式設定為支援 iOS/iPadOS DEP 裝置。

1. 在 [Microsoft 端點管理員系統管理中心](#)，移至 > [所有 應用程式 > 新增] 來新增Intune 公司入口網站 應用程式。
2. 移至 [應用程式 > 應用程式設定原則]，為公司入口網站應用程式建立應用程式設定原則。
3. 使用下列 XML 建立應用程式設定原則。如需如何建立應用程式設定原則並輸入 XML 資料的詳細資訊，請參閱 [為受控 iOS/iPadOS 裝置新增應用程式設定原則](#)。

- 在使用使用者親和性註冊的自動裝置註冊 (ADE) 裝置上使用公司入口網站：

NOTE

當註冊設定檔將 [] 設定為 [是] 時，Intune會在初始註冊程式中自動推送下列應用程式設定原則。此設定不應手動部署至使用者或裝置，因為這會導致與註冊期間已傳送的承載發生衝突，導致使用者在登入公司入口網站 (之後，要求他們下載新的管理設定檔，因為這些裝置上已安裝管理設定檔)。

```
<dict>
  <key>IntuneCompanyPortalEnrollmentAfterUDA</key>
  <dict>
    <key>IntuneDeviceId</key>
    <string>{{deviceid}}</string>
    <key>UserId</key>
    <string>{{userid}}</string>
  </dict>
</dict>
```

- 在未註冊使用者親和性的 DEP 裝置上使用公司入口網站 (也稱為裝置預備)：

NOTE

登入公司入口網站的使用者會設定為裝置的主要使用者。

```
<dict>
  <key>IntuneUDAUserlessDevice</key>
  <string>{{SIGNEDDEVICEID}}</string>
</dict>
```

4. 使用以所需群組為目標的應用程式設定原則，將公司入口網站部署至裝置。請務必將原則部署至已註冊 DEP 的裝置群組。
5. 告知使用者在應用程式自動安裝時登入公司入口網站應用程式。

NOTE

當您新增應用程式組態以允許 DEP 裝置上沒有使用者親和性的公司入口網站應用程式時，您可能會遇到 `STATE Policy Error`。不同于其他應用程式組態，這種情況並不會在每次裝置簽入時套用。相反地，此應用程式組態是一次性作業，可讓在使用者登入公司入口網站時，在沒有使用者親和性的情況下註冊的現有裝置達到使用者親和性。成功套用此應用程式設定之後，就會從背景的原則中移除。原則指派將會存在，但一旦在背景中移除應用程式設定，則不會回報「成功」。應用程式設定原則套用到裝置之後，您就可以取消指派原則。

監視每個裝置的 iOS/iPadOS 應用程式設定狀態

指派設定原則之後，您可以監視每個受管理裝置的 iOS/iPadOS 應用程式設定狀態。從 **Microsoft 端點管理員** [系統管理中心的 [Microsoft Intune](#)]，選取 [所有 > 裝置]。從受控裝置清單中，選取特定裝置以顯示裝置的窗格。在裝置窗格上，選取 [應用程式設定]。

其他資訊

- [部署 iOS/iPadOS 版 Outlook 和 Android 應用程式組態設定](#)

後續步驟

繼續 [指派](#) 和 [監視](#) 應用程式。

新增受控 Android Enterprise 裝置的應用程式設定原則

2022/9/27 •

中的應用程式設定原則Microsoft Intune提供受控 Android Enterprise 裝置上受控 Google Play 應用程式的設定。應用程式開發人員會公開 Android 管理的應用程式組態設定。Intune使用這些公開設定，讓系統管理員設定應用程式的功能。應用程式設定原則會指派給您的使用者群組。原則設定會在應用程式檢查時使用，通常是應用程式第一次執行時。

並非每個應用程式都支援應用程式設定。請與應用程式開發人員確認其應用程式是否支援應用程式設定原則。

NOTE

Intune需要 Android 8.x 或更新版本才能進行裝置註冊案例，以及透過受控裝置應用程式設定原則傳遞的應用程式設定。此需求不適用於 [Microsoft Teams Android 裝置](#)，因為這些裝置將繼續受到支援。

針對Intune應用程式保護原則和透過 Managed 應用程式應用程式設定原則傳遞的應用程式設定，Intune需要 Android 9.0 或更新版本。

電子郵件應用程式

Android Enterprise有數種註冊方法。註冊類型取決於在裝置上設定電子郵件的方式：

- 在 Android Enterprise完全受控、專用和公司擁有的工作設定檔上，使用應用程式設定原則和本文中的步驟。應用程式設定原則支援 Gmail 和 Nine Work 電子郵件應用程式。
- 在 Android Enterprise具有工作設定檔的個人擁有裝置上，建立[Android Enterprise電子郵件裝置組態設定檔](#)。當您建立設定檔時，可以設定支援應用程式設定原則之電子郵件用戶端的設定。使用設定設計工具時，Intune 包含 Gmail 和 Nine Work 應用程式專屬的電子郵件設定。
- 在 Android 裝置系統管理員上，為 Samsung Knox 裝置建立 [Android 裝置系統管理員電子郵件裝置組態設定檔](#)。當您建立設定檔時，可以設定Exchange電子郵件設定，例如 `outlook.office365.com`。

建立應用程式設定原則

- 登入 [Microsoft 端點管理員系統管理中心](#)。
- 選擇 [應用程式 >] [應用程式設定原則 >] [新增 >] [受控裝置]。請注意，您可以在受控裝置 和受控應用程式 之間進行選擇。如需詳細資訊，請參閱[支援應用程式設定的應用程式](#)。
- 在 [基本] 頁面上，設定下列詳細資料：
 - 名稱 - 出現在入口網站中的設定檔名稱。
 - 描述 - 顯示在入口網站中的設定檔描述。
 - 裝置註冊類型 - 此設定設為受控裝置。
- 選取 [Android Enterprise] 作為 [平臺]。
- 按一下 [目標應用程式] 旁的 [選取應用程式]。[相關聯的應用程式] 窗格隨即顯示。
- 在 [相關聯的應用程式] 窗格中，選擇要與設定原則相關聯的受控應用程式，然後按一下 [確定]。
- 按一下 [下一步] 以顯示 [設定] 頁面。
- 按一下 [新增] 以顯示 [新增許可權] 窗格。

9. 按一下您要覆寫的許可權。授與的許可權將會覆寫所選應用程式的「預設應用程式許可權」原則。
10. 設定每個 許可權 的許可權狀態。您可以從 [提示]、[自動授與] 或 [自動拒絕] 中選擇。
11. 如果受控應用程式支援組態設定，則會顯示 [組態 設定格式] 下拉式方塊。選取下列其中一個方法來新增組態資訊：
 - 使用設定設計工具
 - 輸入 JSON 資料如需使用設定設計工具的詳細資訊，請 [參閱使用設定設計工具](#)。如需輸入 XML 資料的詳細資訊，請 [參閱輸入 JSON 資料](#)。
12. 如果您需要讓使用者跨工作和個人設定檔連接目標應用程式，請選取 [已連線的應用程式] 旁的 [啟用]。

Home > Apps >

Create app configuration policy ...

1 Basics 2 Settings 3 Assignments 4 Review + create

Permissions

Permissions granted here will override the "Default app permissions" policy for the selected apps.

[Learn more about Android runtime permissions](#)

+Add

Not configured

Configuration Settings

Configuration settings format ⓘ Select one ▼

Connected apps

Enable users to connect this app across the work and personal profiles ⓘ

Enabled Not configured

This setting only works for corporate-owned work profile devices. [Learn more about connected apps](#)

Previous Next

NOTE

此設定僅適用於個人擁有的工作設定檔和公司擁有的工作設定檔裝置。

將 [] 設定變更為 [] 不會從裝置移除設定原則。若要從裝置移除 功能，您必須取消指派相關的設定原則。

13. 按 [下一步] 以顯示 [指派] 頁面。
14. 在 [指派給] 旁的下拉式方塊中，選取 [選取的群組]、[所有使用者]、[所有裝置] 或 [所有使用者和所有開發人員] 來指派應用程式設定原則。

Included groups

Assign to

Selected groups



Selected groups

No groups selected

[+ Select groups to include](#)

Excluded groups



When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more.](#)

Selected groups

No groups selected

[+ Select groups to exclude](#)

Previous

Next

15. 在下拉式方塊中選取 [所有使用者]。

Create app configuration policy

✓ Basics ✓ Settings **3 Assignments** 4 Review + create

Included groups

Assign to

All users

Excluded groups

 When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Selected groups

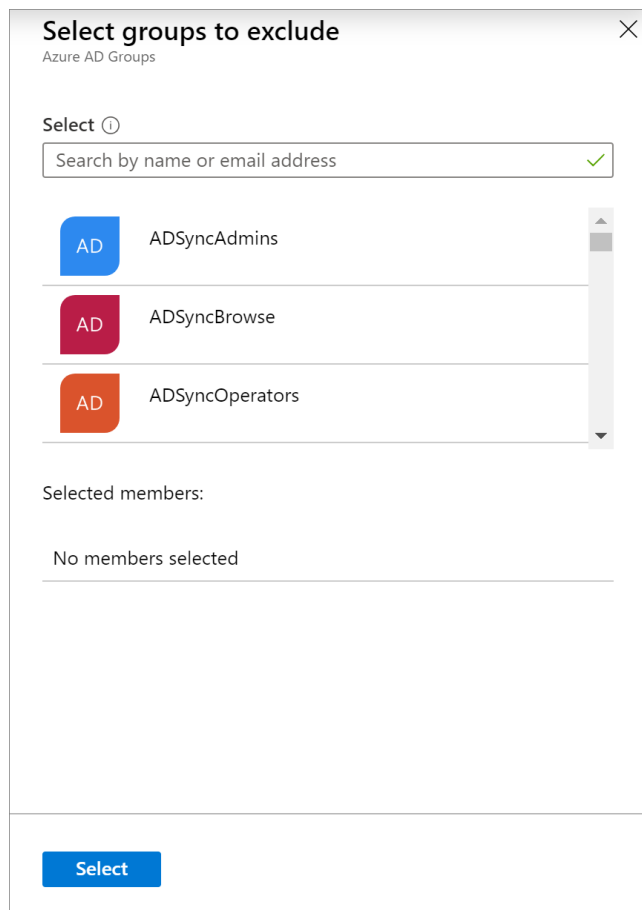
No groups selected

+ [Select groups to exclude](#)

Previous

Next

16. 按一下 [選取要排除的群組] 以顯示相關窗格。



17. 選擇您想要排除的群組，然後按一下 [選取]。

NOTE

新增群組時，如果指定的指派類型已包含任何其他群組，則會預先選取該群組，而且對於其他 include 指派類型則無法變更。因此，該群組已使用，不能當做排除的群組使用。

18. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。
19. 按一下 [建立] 將應用程式設定原則新增至Intune。

使用設定設計工具

當應用程式設計為支援組態設定時，您可以使用受控 Google Play 應用程式的設定設計工具。設定適用於在 Intune 中註冊的裝置。設計工具可讓您為應用程式公開的設定設定特定組態值。

1. 選取 ****[新增]。選擇您要為應用程式輸入的組態設定清單。

如果您使用 Gmail 或 Nine Work 電子郵件應用程式，[Android Enterprise裝置設定來設定電子郵件](#)，會有這些特定設定的詳細資訊。

2. 針對組態中的每個索引鍵和值，設定：

- **數值型別**：組態值的資料類型。針對字串實數值型別，您可以選擇選擇變數或憑證設定檔作為實數值型別。
- **組態值**：組態的值。如果您選取 [值] 類型的變數或憑證，請從變數或憑證配置檔案清單中選擇。如果您選擇憑證，則會在執行時間填入部署至裝置之憑證的憑證別名。

組態值支援的變數

如果您選擇變數作為實數值型別，您可以選擇下列選項：

「	「
Azure AD裝置識別碼	dc0dc142-11d8-4b12-bfea-cae2a8514c82
帳戶識別碼	fc0dc142-71d8-4b12-bbea-bae2a8514c81
Intune裝置識別碼	b9841cd9-9843-405f-be28-b2265c59ef97
網域	contoso.com
郵件	john@contoso.com
部分 UPN	約翰
使用者識別碼	3ec2c00f-b125-4519-acf0-302ac3761822
使用者名稱	無名氏
使用者主體名稱	john@contoso.com

只允許應用程式中已設定的組織帳戶

身為Microsoft Intune系統管理員，您可以控制要將哪些公司或學校帳戶新增至受管理裝置上的 Microsoft 應用程式。您可以限制只能存取允許的組織使用者帳戶，並封鎖已註冊裝置上的個人帳戶。針對 Android 裝置，請在受控裝置應用程式設定原則中使用下列機碼/值組：

「	COM.MICROSOFT.INTUNE.MAM.ALLOWEDACCOUNTUPNS
■	- 一或多個 <code>；</code> 分隔的 UPN。 - 唯一允許的帳戶是由此機碼所定義的受管使用者帳戶。 - 針對Intune註冊的 <code>{{userprincipalname}}</code> 裝置，可以使用權杖來代表已註冊的使用者帳戶。

NOTE

下列應用程式會處理上述應用程式設定，且只允許組織帳戶：

- Android 版 Edge (42.0.4.4048 和更新版本)
- Office、Word、Excel、Android 版 PowerPoint (16.0.9327.1000 和更新版本)
- Android (5.28 和更新版本的OneDrive)
- Android 版 OneNote (16.0.13231.20222 或更新版本)
- Android (2.2.222 和更新版本的Outlook)
- Android (1416/1.0.0.2020073101 和更新版本的) Teams

輸入 JSON 資料

(應用程式上的某些組態設定，例如) 套件組合類型的應用程式，無法使用設定設計工具進行設定。針對這些值使用 JSON 編輯器。設定會在安裝應用程式時自動提供給應用程式。

- 針對 [組態設定格式]，選取 [輸入 JSON 編輯器]。
- 在編輯器中，您可以定義組態設定的 JSON 值。您可以選擇 [下載 JSON 範本] 來下載範例檔案，然後再進行設定。

3. 選擇 [確定]，然後選擇 [新增]。

原則會建立並顯示在清單中。

當指派的應用程式在裝置上執行時，它會以您在應用程式設定原則中設定的設定執行。

啟用已連線的應用程式

適用於：

Android 11+

個人擁有的工作設定檔使用者必須公司入口網站 5.0.5291.0 版或更新版本。公司擁有的工作設定檔使用者不需要特定版本的Microsoft Intune應用程式來提供支援。

您可以允許使用者使用 Android 個人擁有和公司擁有的工作設定檔，為支援的應用程式開啟連線的應用程式體驗。此應用程式組態設定可讓應用程式跨工作和個人應用程式實例連線及整合應用程式資料。

若要讓應用程式提供此體驗，應用程式必須與 Google 的連線應用程式 SDK 整合，因此只有有限的應用程式支援它。您可以主動開啟連線的應用程式設定，而當應用程式新增支援時，使用者將能夠啟用連線的應用程式體驗。

將 [已連線的應用程式] 設定變更為 [未設定] 不會從裝置移除設定原則。若要從裝置移除 連線的應用程式 功能，您必須取消指派相關的設定原則。

WARNING

如果您啟用應用程式的連線應用程式功能，個人應用程式中的工作資料將不會受到應用程式保護原則的保護。

此外，不論您連線的應用程式設定為何，某些 OEM 可能會自動連線特定應用程式，或是能夠要求使用者核准來連線您未設定的應用程式。在此案例中，應用程式的範例可能是 OEM 的鍵盤應用程式。

在您啟用已連線的應用程式設定之後，使用者有兩種方式可以連線到公司和個人應用程式：

1. 支援的應用程式可以選擇提示使用者核准跨設定檔進行連線。
2. 使用者可以開啟設定應用程式，並移至 [已連線的工作&個人應用程式] 區段，其中會看到列出所有支援的應用程式。

IMPORTANT

如果針對以相同裝置為目標的相同應用程式指派多個應用程式設定原則，而其中一個原則將 [ Enabled] 設定為，而另一個原則則不會，則應用程式組態會報告衝突，而在裝置上套用的結果行為將會是不允許連線的應用程式。

預先設定應用程式的許可權授與狀態

您也可以預先設定應用程式許可權，以存取 Android 裝置功能。根據預設，需要裝置許可權的 Android 應用程式，例如位置或裝置相機的存取權，會提示使用者接受或拒絕許可權。

例如，應用程式會使用裝置的麥克風。系統會提示使用者授與應用程式使用麥克風的許可權。

1. 在 [Microsoft 端點管理員系統管理中心](#)，選取 [應用程式**][應用程式** > 設定原則 >][新增 >][受控裝置]。
2. 新增下列屬性：

- **名稱**：輸入原則的描述性名稱。為您的設定檔命名，以方便之後能夠輕鬆識別。例如，良好的原則名稱是 Android Enterprise 整家公司的提示許可權應用程式原則。
- **描述**：輸入設定檔的描述。這是選擇性設定，但建議進行。
- **裝置註冊類型**：此設定設為受控裝置。
- **平臺**：選取 [Android Enterprise]。

3. 選取 [配置檔案類型]：
4. 選取 [目標應用程式]。選擇您要與設定原則建立關聯的應用程式。從已核准並與Intune同步處理的Android Enterprise完全受控工作設定檔應用程式清單中選取。
5. 選取 [許可權 >][新增]。從清單中, 選取 [確定] > 可用的應用程式權限。
6. 針對要使用此原則授與的每個許可權選取一個選項：
 - 提示。提示使用者接受或拒絕。
 - 自動授與。自動核准而不通知使用者。
 - 自動拒絕。自動拒絕而不通知使用者。
7. 若要指派應用程式設定原則, 請選取 [指派 >][選取群組] > 應用程式設定原則。選擇要指派的使用者群組 > 選取]。
8. 選擇 [儲存] 以指派原則。

其他資訊

- [將受控 Google Play 應用程式指派給 Android Enterprise個人擁有和公司擁有的工作設定檔裝置](#)
- [部署 iOS/iPadOS 和 Android 應用程式組態設定的Outlook](#)

後續步驟

繼續 [指派](#) 和 [監視](#) 應用程式。

Intune App SDK 受控應用程式的應用程式設定原則

2022/9/27 •

Intune App Software Development Kit (SDK) 支援透過行動應用程式管理 (MAM) 通道傳遞應用程式設定。在 Intune 入口網站中，MAM 通道稱為受控應用程式應用程式設定原則。MAM 通道不同于註冊裝置時所提供的行動裝置管理 (MDM) OS 平臺通道。

若要透過 MAM 通道支援應用程式設定，應用程式必須與 [Intune App SDK](#) 整合。企業營運應用程式可以整合 Intune App SDK 或使用 [Intune App Wrapping Tool](#)。如需 Intune App SDK 與 Intune App Wrapping Tool 之間的比較，請參閱 [準備應用程式保護原則的企業營運應用程式](#)。

使用 MAM 通道，無論裝置註冊狀態為何，應用程式都可以接收應用程式設定原則。如需哪些應用程式透過 MAM 通道支援應用程式設定的相關資訊，請參閱 [Microsoft Intune 受保護的應用程式](#)。您應該檢閱應用程式廠商的檔，以查看可用的設定，以及設定如何影響應用程式的行為。

如需詳細資訊，請參閱 [適用於 Microsoft Intune 的應用程式設定原則](#)。

NOTE

Intune 需要 Android 8.x 或更新版本才能進行裝置註冊案例，以及透過受控裝置應用程式設定原則傳遞的應用程式設定。此需求不適用於 [Microsoft Teams Android 裝置](#)，因為這些裝置將繼續受到支援。

針對 Intune 應用程式保護原則和透過 Managed 應用程式應用程式設定原則傳遞的應用程式設定，Intune 需要 Android 9.0 或更新版本。

新增受控應用程式應用程式設定原則

使用下列步驟來建立受控應用程式應用程式設定原則。建立組態之後，您可以將其設定指派給使用者群組。

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選擇 [應用程式 > 應用程式設定原則 >][新增 > Managed 應用程式]。
3. 在 [基本] 頁面上，設定下列詳細資料：
 - **名稱**：將出現在入口網站中的設定檔名稱。
 - **描述**：將出現在入口網站中的設定檔描述。
 - **裝置註冊類型**：已選取受控應用程式。
4. 選擇 [選取公用應用程式] 或 [選取自訂應用程式] 以選擇您要設定的應用程式。從您已核准並與 Intune 同步處理的應用程式清單中選取應用程式。
5. 按一下 [下一步] 以顯示 [設定] 頁面。
6. [設定] 頁面 會根據您要設定的應用程式，提供顯示的選項：
 - **一般組態設定** - 針對應用程式支援的每個一般組態設定，輸入 [名稱] 和 [值]。

Intune 啟用 App SDK 的應用程式支援機碼/值組中的設定。若要深入瞭解支援哪些機碼/值組態，請參閱每個應用程式的檔。請注意，您可以使用會動態填入應用程式所產生資料的權杖。若要刪除一般組態設定，請選擇省略號 (...)，然後選取 [刪除]。如需詳細資訊，請參閱 [使用權杖的組態值](#)。

如需特定 Microsoft 應用程式的應用程式組態設定相關資訊，請參閱：

- 使用適用於 iOS 和 Android 的 Edge 搭配 Microsoft Intune 來管理 Web 存取
- 使用 Microsoft Intune 管理適用於 iOS 和 Android 的 Office 共同作業體驗
- 部署適用於 iOS 和 Android 的 Outlook 應用程式組態設定
- 使用 Microsoft Intune 在 iOS 和 Android 版 Teams 中管理共同作業體驗

7. 按 [下一步] 以顯示 [指派] 頁面。
8. 按一下 [選取要包含的群組]。
9. 在 [選取要包含的群組] 窗格中選取群組，然後按一下 [選取]。
10. 按一下 [選取要排除的群組] 以顯示相關窗格。
11. 選擇您想要排除的群組，然後按一下 [選取]。

NOTE

新增群組時，如果指定的指派類型已包含任何其他群組，則會預先選取該群組，而且對於其他 include 指派類型則無法變更。因此，該群組已使用，不能當做排除的群組使用。

12. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。
13. 按一下 [建立] 將應用程式設定原則新增至Intune。

使用權杖的組態值

Intune可以產生特定權杖，並將其傳送至 Managed 應用程式。例如，如果您的應用程式組態可以使用電子郵件設定，您可以使用權杖來新增動態電子郵件。在 [名稱] 欄位中輸入應用程式預期的名稱，然後在 [值] 欄位中輸入 `{{mail}}`。

Intune組態設定中支援下列權杖類型。不支援其他自訂索引鍵/值組。

- `{{userprincipalname}}` —例如，John@contoso.com
- `{{mail}}` —例如，John@contoso.com
- `{{partialupn}}` -例如 John
- `{{accountid}}` —例如 fc0dc142-71d8-4b12-bbea-bae2a8514c81
- `{{userid}}` —例如 3ec2c00f-b125-4519-acf0-302ac3761822
- `{{username}}` —例如 John Doe
- `{{PrimarySMTPAddress}}` —例如，testuser@ad.domain.com

NOTE

和 `{{}}` 字元僅供權杖類型使用，不得用於其他用途。

後續步驟

如往常一樣繼續 [指派](#) 和 [監視](#) 應用程式。

使用 iOS 應用程式布建設定檔，以防止應用程式到期

2022/9/27 •

簡介

Apple iOS/iPadOS 指派給 iPhone 和 iPad 的企業營運應用程式，是以包含的布建設定檔和使用憑證簽署的程式碼所建立。當應用程式執行時，iOS/iPadOS 會確認 iOS/iPadOS 應用程式的完整性，並強制執行提供設定檔所定義的原則。會進行下列驗證：

- **安裝檔完整性** -iOS/iPadOS 會將應用程式的詳細資料與企業簽署憑證的公開金鑰進行比較。如果兩者不同，應用程式的內容可能已變更，且不允許執行應用程式。
- **功能強制執行** -iOS/iPadOS 會嘗試強制執行從 enterprise 布建設定檔 (的應用程式功能，而不是應用程式安裝 (ipa) 檔中的個別開發人員布建設定檔)。

您用來簽署應用程式的企業簽署憑證通常會持續三年。不過，置備設定檔會在一年後到期。當憑證仍然有效時，Intune 會提供工具，以主動將新的布建設定檔指派給具有接近到期之應用程式的裝置。憑證到期後，您必須使用新的憑證重新簽署應用程式，並將新的布建設定檔與新憑證的金鑰內嵌在一起。

作為系統管理員，您可以加入和排除安全性群組，以指派 iOS/iPadOS 應用程式布建設定。例如，您可以將 iOS/iPadOS 應用程式布建設定指派給所有使用者，但不包括 executive 群組。

如何建立 iOS 行動應用程式布建設定檔

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 **應用 > 程式 iOS 應用程式 > 布 建設定檔建立設定檔**。
3. 在 [基礎] 頁面上，新增下列值：
 - **Name** -提供此行動提供設定檔的名稱。
 - **Description** - (選用) 提供原則的描述。
 - **Upload 設定檔 檔**-選擇 [開啟 圖示]，然後選擇 [apple 行動裝置設定] 設定檔檔案 (，並以您從 [Apple 開發人員網站](#) 下載的副檔名 `.mobileprovision`) 進行。

到期日 會從您在上面新增的 Apple 行動裝置設定檔檔案中的值填入。

Home > Microsoft Intune > Client apps - iOS app provisioning profiles > Create profile

Create profile ✕

Basics

Scope tags

Assignments

Review + create

Name *

Description

Upload profile file

Select an iOS provisioning profile 

Expiration date

Review + create

Previous

Next: Scope tags >

4. 按 [下一步: 範圍標記]。

在 [範圍 標籤] 頁面上, 您可以選擇設定範圍標記, 判斷誰可以查看 Intune 中的 iOS/iPadOS 應用程式布建設定檔。如需有關範圍標籤的詳細資訊, 請參閱 [使用角色型存取控制和範圍標籤來發佈它](#)。

5. 按 [下一步: 工作分派]。

[工作分派] 頁面可讓您將設定檔指派給使用者和裝置。請務必注意, 不論裝置是否由 Intune 所管理, 您都可以將設定檔指派給裝置。

6. 按 [下一步: 複查 + 建立] 以檢查您為設定檔輸入的值。

7. 完成後, 按一下 [建立], 以在 Intune 中建立 iOS/iPadOS 應用程式布建設定檔。

後續步驟

將設定檔指派給必要的 iOS/iPadOS 裝置。如需詳細資訊, 請使用 [如何指派裝置設定檔](#) 的步驟。

設定適用於 Android Enterprise 的 Microsoft 受控主畫面應用程式

2022/9/27 •

受控主畫面是公司擁有的 Android 應用程式，Enterprise 透過 Intune 註冊並以多應用程式 kiosk 模式執行的專用裝置。對於這些裝置，受控主畫面會作為啟動器，讓其他核准的應用程式在上面執行。受控主畫面可讓 IT 系統管理員自訂其裝置，並限制終端使用者可以存取的功能。如需詳細資訊，請參閱 [如何在多應用程式 Kiosk 模式的專用裝置上設定 Microsoft 受控主畫面](#)。

設定 Microsoft 受控主畫面應用程式的時機

首先，請確定您的裝置受到支援。Intune 支援針對執行 OS 8.0 版和更新版本且可靠地連線到 Google 行動服務的 Android 裝置註冊 Android Enterprise 專用裝置。同樣地，受控主畫面支援執行 OS 8.0 版和更新版本的 Android 裝置。

一般而言，如果可透過裝置組態取得設定，請在該處設定設定。這樣做可節省時間、將錯誤降至最低，並提供更好的 Intune 支援體驗。不過，某些 Managed Home Screen 設定目前只能透過 Intune 主控台中的 [應用程式 設定原則] 窗格來使用。使用本檔瞭解如何使用設定設計工具或 JSON 腳本來設定不同的設定。此外，請使用本檔來瞭解哪些受控主畫面設定可使用裝置組態。您也可能會看到 [專用裝置設定](#)，以取得會影響受控主畫面的裝置組態中可用的完整設定清單。

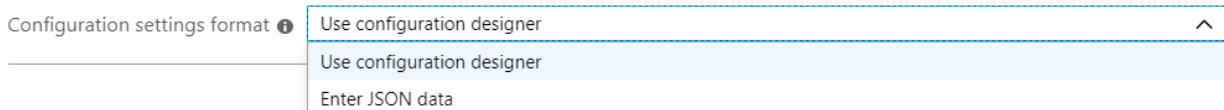
如果使用應用程式設定，請流覽至 [Microsoft 端點管理員系統管理中心](#)，然後選取 [應用程式**][應用程式** > 設定原則]。為執行 Android 的受管理裝置新增設定原則，然後選擇 [受控主畫面] 作為相關聯的應用程式。選取 [組態設定] 以設定不同的可用受控主畫面設定。

選擇設定設定格式

您可以使用兩種方法來定義受控主畫面的組態設定：

- **設定設計工具** 可讓您使用容易使用的 UI 來設定設定，讓您開啟或關閉功能並設定值。在此方法中，有幾個停用的組態索引鍵具有實數值型別 `BundleArray`。這些設定金鑰只能藉由輸入 JSON 資料來設定。
- **JSON 資料** 可讓您使用 JSON 腳本定義所有可能的組態金鑰。

如果您使用設定設計工具新增屬性，您可以從 [組態 設定格式] 下拉式清單中選取 [輸入 JSON 資料]，自動將這些屬性轉換成 JSON。



使用設定設計工具

設定設計工具可讓您選取預先填入的設定及其相關聯的值。

Add

CONFIGURATION KEY	VALUE TYPE	CONFIGURATION VALUE	DESCRIPTION
Show Bluetooth setting	bool	false	Show Bluetooth setting
Show Wi-Fi setting	bool	false	Show Wi-Fi setting
Exit lock task mode password	string	1234	Exit lock task mode password
Battery and Signal Strength ...	bool	true	Battery and Signal Strength indica...

下表列出 Managed Home Screen 可用的組態索引鍵、數值型別、預設值和描述。描述會根據選取的值提供預期的裝置行為。設定設計工具中已停用 類型的 `BundleArray` 組態金鑰，本檔的 `Enter JSON Data` 一節會進一步說明。

設定來自訂受控主畫面的應用程式、資料夾和一般外觀：

NAME	VALUE TYPE	DESCRIPTION	DEFAULT VALUE	STATUS
設定允許列出的應用程式	bundleArray	請參閱本檔的 JSON 一節。	可讓您從裝置上安裝的應用程式中，定義一組可在主畫面上顯示的應用程式。您可以輸入您想要顯示之應用程式的應用程式套件名稱來定義應用程式。例如， <code>com.microsoft.emmx</code> 會讓設定可在主畫面上存取。您在本節中允許列出的應用程式應該已安裝在裝置上，才能顯示在主畫面上。	✓
設定釘選的 Web 連結	bundleArray	請參閱本檔的 JSON 一節。	可讓您將網站釘選為主畫面上的快速啟動圖示。使用此設定，您可以定義 URL，並將其新增至主畫面，讓終端使用者在瀏覽器中單次點選即可啟動。注意：建議您建立、指派及核准裝置的受控 Google Play Web 連結。當您這麼做時，它們會被視為允許列出的應用程式。	✓

名稱	類型	預設值	說明	狀態
建立用於群組應用程式的受控資料夾	bundleArray	請參閱本檔的 JSON 格式 一節。	可讓您在這些資料夾內建立及命名資料夾和群組應用程式。終端使用者無法移動資料夾、重新命名資料夾、或移動資料夾內的應用程式。資料夾會以建立的順序出現，而資料夾內的應用程式會依字母順序顯示。注意：您想要群組到資料夾中的所有應用程式都必須視需要指派給裝置，而且必須已新增至受控主畫面。	✓
設定格線大小	字串	自動	可讓您設定要在受控主畫面上放置應用程式的格線大小。您可以設定應用程式資料列和資料行的數目，以下列格式定義格線大小： <code>columns;rows</code> 。如果您定義格線大小，則主畫面上資料列中顯示的應用程式數目上限是您設定的資料列數目。主畫面中資料行中顯示的應用程式數目上限是您設定的資料行數目。	✓
鎖定主畫面	bool	TRUE	移除使用者在主畫面上移動應用程式圖示的能力。如果您啟用此設定金鑰，主畫面上的應用程式圖示會鎖定。終端使用者無法拖放到主畫面上的不同格線位置。如果變成 false，終端使用者可以在 Managed Home Screen 上四處移動應用程式和 Web 連結圖示。	✓
已啟用應用程式順序	bool	假	將此設定轉換為 True 可讓您設定 Managed Home Screen 上應用程式、Web 連結和資料夾的順序。啟用之後，請使用 app_order 設定排序。	✓

項目	型別	預設值	說明	支援狀態
應用程式順序	bundleArray	請參閱本檔的 JSON 格式 一節。	可讓您在 Managed Home Screen 上指定應用程式、Web 連結和資料夾的順序。若要使用此設定，必須啟用鎖定主畫面、必須定義 [設定格線大小]，且 [啟用應用程式順序] 必須設定為 [True]。	✓
資料夾中的應用程式會依名稱排序	bool	TRUE	False 允許資料夾中的專案以指定的順序顯示。否則，它們會依字母順序出現在資料夾中。	✗
設定應用程式圖示大小	整數	2	可讓您為主畫面上顯示的應用程式設定圖示大小。您可以在此組態中針對不同的大小選擇下列值 - 0 (最小)、1 (Small)、2 (一般)、3 (大型) 和 4 (最大)。	✓
設定應用程式資料夾圖示	整數	0	可讓您定義主畫面上應用程式資料夾的外觀。您可以從下列值選擇外觀：深色方形 (0)；深色圓形 (1)；淺色方 (2)；淺色圓形 (3)。	✓
設定螢幕方向	整數	1	可讓您將主畫面的方向設定為直向模式、橫向模式或允許自動旋轉。您可以輸入直向模式) 值 1 (、橫向模式) 輸入 2 (、自動路由) 輸入 3 (來設定方向。	✓
設定裝置牆紙	字串	預設	可讓您設定您選擇的桌布。輸入您要設定為桌布的影像 URL。	✓
定義主題色彩	字串	光	指定您要讓受控主畫面以「淺色」或「深色」模式執行。	✗

裝置周邊和 Managed Home Screen 設定的組態：

項目	型別	預設值	說明	支援狀態

設定名稱	資料類型	預設值	說明	驗證狀態
顯示 Managed 設定	bool	TRUE	「受控設定」是受控主畫面應用程式，只有在您已設定任何快速存取設定時才會出現。這些設定可以包括 [顯示Wi-Fi設定]、[顯示藍牙] 設定、[顯示磁片區] 設定，以及 [顯示手電筒筒] 設定。您也可以透過在螢幕上向下撥動來存取這些設定。將此金鑰設定為 False 可隱藏「受控設定」應用程式，並讓使用者只能透過向下撥動來存取設定。	✓
顯示Wi-Fi設定	bool	假	將此設定轉換為 True 可讓終端使用者連線到不同的Wi-Fi網路。	✓
啟用Wi-Fi允許清單	bool	假	True 是表示 填寫Wi-Fi允許清單金鑰，以限制受控主畫面中顯示的Wi-Fi網路。設定為 False 以顯示裝置探索到的所有可能Wi-Fi網路。只有在顯示Wi-Fi設定已設定為 True 且已填入Wi-Fi允許清單時，此設定才相關。	✓
Wi-Fi允許清單	bundleArray	請參閱本檔的 ■ JSON ■ 一節。	可讓您列出您希望裝置在 Managed Home Screen 中顯示Wi-Fi網路的所有 SSID。只有當 [顯示Wi-Fi] 設定和 [啟用Wi-Fi允許清單] 設定為 [True] 時，此清單才相關。如果任一設定已設定為 False，則您不需要修改此組態。	✓
顯示藍牙設定	bool	假	將此設定設為 True 可讓終端使用者開啟或關閉藍牙，並聯機到支援藍牙的不同裝置。	✓
顯示磁片區設定	bool	假	將此設定切換為 True 可讓使用者存取磁片區滑杆來調整媒體音量。	✓

項目	類型	預設值	說明	驗證結果
顯示手電筒設定	bool	假	將此設定設為 True 可讓終端使用者開啟或關閉裝置的手電筒。如果裝置不支援手電筒，則即使設定為 True，也不會顯示此設定。	✓
顯示裝置資訊設定	bool	假	True 可讓使用者從受控設定應用程式或向下撥動存取裝置的快速資訊。無障礙資訊包括 OS 8 的裝置製造、型號和序號。	✓
在 MHS 上顯示裝置的名稱	bool	假	將此設定轉換為 True，即可輕鬆地從受控設定應用程式檢視裝置Intune入口網站的「裝置名稱」屬性，或在 [] 設為 [True] 時從向下撥動。請務必也包含字串屬性「Device's name」，這是由具有正確值的 Intune自動填入。	✗
顯示 MHS 上所有支援 OS 版本的序號	選擇	{{serialnumber}}	確定應用程式內設定 device_serial_number 已設定為顯示 {{SerialNumber}} [] 設為 [True]。這個值會由具有正確值的 Intune自動填入。	✗
啟用虛擬首頁按鈕	bool	假	True 可讓終端使用者存取受控主畫面首頁按鈕，該按鈕會從使用者目前的工作返回受控主畫面。	✓
虛擬首頁按鈕的類型	字串	swipe_up	使用swipe_up以向上撥動手勢存取首頁按鈕。使用 float 存取可由終端使用者在螢幕上移動的黏性、永續性首頁按鈕。	✓

項目	類型	預設值	說明	狀態
啟用通知徽章	bool	假	啟用應用程式圖示的通知徽章，以顯示應用程式上的新通知數目。如果啟用此設定，終端使用者會在具有未讀取通知的應用程式上看到通知徽章。如果您將此組態金鑰保持停用，終端使用者將不會看到任何可能具有未讀取通知的應用程式收到徽章的通知。	✓
電池和訊號強度指標列	bool	TRUE	將此設定轉換為 True 會顯示電池和訊號強度指標列。	✗

IMPORTANT

受控主畫面應用程式已在 API 層級更新，以更符合 Google Play 商店的需求。如此一來，Wi-Fi組態在受控主畫面中的運作方式有一些變更。變更包括下列專案：

- 無法變更 (啟用或停用) 裝置的Wi-Fi連線。使用者將能夠在網路之間切換，但無法開啟/關閉 Wi-Fi。
- 無法自動連線到第一次需要密碼的已設定Wi-Fi網路。設定的網路會在第一次輸入密碼之後自動連線。

在執行 OS 11 的 Android 裝置上，當使用者嘗試透過受控主畫面應用程式連線到網路時，系統會提示使用者同意快顯視窗。此快顯視窗來自 Android 平臺，並非受控主畫面應用程式專用。此外，當使用者嘗試透過受控主畫面應用程式連線到受密碼保護的網路時，系統會要求他們輸入密碼。即使密碼正確，只有在裝置未連線到網路時，網路才會變更。已連線到穩定網路的裝置將無法透過受控主畫面應用程式連線到受密碼保護的網路。

在執行 OS 10 的 Android 裝置上，當使用者嘗試透過受控主畫面應用程式連線到網路時，系統會透過通知提示他們同意。由於此提示，OS 10 上的使用者必須能夠存取狀態列和通知，才能完成同意步驟。如有需要，請使用 [專用裝置的 \[一般\] 設定](#)，讓狀態列和通知可供使用者使用。此外，當使用者嘗試透過受控主畫面應用程式連線到受密碼保護的網路時，系統會要求他們輸入密碼。即使密碼正確，只有在裝置尚未連線到穩定網路時，網路才會變更。

自訂螢幕保護裝置程式的設定：

項目	類型	預設值	說明	狀態
啟用螢幕保護裝置	bool	假	啟用螢幕保護裝置模式。如果設定為 true，您可以設定 screen_saver_image、screen_saver_show_time、inactive_time_to_show_screen_saver和 media_detect_screen_saver。	✓

項目	類型	預設值	說明	驗證結果
螢幕保護裝置影像	字串		設定螢幕保護裝置影像的 URL。如果未設定 URL, 裝置會在啟用螢幕保護裝置時顯示預設螢幕保護裝置影像。預設影像會顯示 Managed Home Screen 應用程式圖示。	✓
螢幕保護裝置顯示時間	整數	0	提供選項以秒為單位設定裝置在螢幕保護裝置模式期間顯示螢幕保護的時間量。如果設定為 0, 螢幕保護裝置會無限期中顯示在螢幕保護裝置模式上, 直到裝置變成作用中為止。	✓
啟用螢幕保護裝置的非使用中時間	整數	30	裝置在觸發螢幕保護裝置程式之前處於非作用中的秒數。如果設定為 0, 裝置將永遠不會進入螢幕保護裝置模式。	✓
顯示幕幕保護之前, 媒體偵測	bool	TRUE	選擇裝置畫面是否應該在裝置上播放音訊/視訊時顯示幕幕保護。如果設定為 true, 裝置將不會播放音訊/視訊, 不論 inactive_time_to_show_screener 中的值為何。如果設定為 false, 裝置畫面會根據 inactive_time_to_show_screen_saver 中設定的值來顯示幕幕保護。	✓

NOTE

每當鎖定畫面出現時, Managed Home Screen 就會啟動畫面保護。如果系統的鎖定畫面逾時時間超過 Screenaver 10 分鐘, 則螢幕保護裝置會顯示到鎖定畫面出現為止。如果系統的鎖定畫面逾時比 10 分鐘, 螢幕保護裝置就會在裝置的鎖定畫面出現時立即出現。

可協助對裝置問題進行疑難排解的設定：

項目	類型	預設值	說明	驗證結果
結束鎖定工作模式密碼	字串		輸入 4-6 位數的程式碼, 用來暫時退出鎖定工作模式以進行疑難排解。	✓

項目	型別	預設值	說明	驗證結果
啟用輕鬆存取偵錯功能表	bool	假	將此設定轉換為 True 可從 Managed 設定應用程式存取偵錯功能表, 或在 Managed Home Screen 中從向下撥動。偵錯功能表目前是結束 kiosk 模式的功能所在位置, 並可透過按一下 [上一頁] 按鈕約 15 次來存取。將此設定保持為 False, 讓進入點只能透過返回按鈕存取偵錯功能表。	✓
在 MHS 外部啟用最大非使用中時間	bool	假	將此設定轉換為 True, 以在一段設定的閒置期間後自動重新開機 Managed Home Screen。計時器只會計算非使用中時間, 而且在設定時, 每次使用者在 Managed Home Screen 外部與裝置互動時, 都會重設。使用 MHS ■■■ MAX ■■■ 來設定非使用中計時器。根據預設, 此設定已關閉。只有在已設定 ■■■■■ 時, 才能使用此設定。	✗
MHS 外部的最大非使用中時間	整數	180	設定使用者在自動重新開機之前, 可以在 Managed Home Screen 外部花費的最大非使用中時間, 以秒為單位。根據預設, 此設定會設定為 180 秒。■ MHS ■■■■■ 必須設定為 true, 才能使用此設定。	✗
啟用 MHS 外部的最大時間	bool	假	將此設定轉換為 True, 以在經過一段時間後自動重新開機 Managed Home Screen。計時器會將非使用中和使用中的時間納入 Managed Home Screen 外部所花費的時間。使用 MHS ■■■■■ 來設定非使用中計時器。根據預設, 此設定已關閉。只有在已設定 ■■■■■ 時, 才能使用此設定。	✗

名稱	類型	值	說明	預設值
MHS 外部的最大時間	整數	600	設定使用者在自動重新開機之前，可以在 Managed Home Screen 外部花費的最大絕對時間，以秒為單位。根據預設，此組態會設定為 600 秒。■ MHS ■ 必須設定為 true，才能使用此設定。	✗

使用共用裝置模式設定裝置時，自訂受控主畫面體驗的設定 Azure AD：

名稱	類型	值	說明	預設值
啟用登入	bool	假	將此設定轉換為 True 可讓使用者登入 Managed Home Screen。與 Azure AD 共用裝置模式搭配使用時，登入受控主畫面的使用者將會自動登入裝置上已參與 Azure AD 共用裝置模式的所有其他應用程式。此設定預設為關閉。	✓
登入類型	字串	AAD	將此組態設定為「AAD」，以使用 AAD 帳戶登入。否則，請將此組態設定為「Other」。使用非 AAD 帳戶登入的使用者，將不會單一登入已與 Azure AD 共用裝置模式整合，但仍會登入受控主畫面的所有應用程式。根據預設，此設定會使用「AAD」使用者帳戶。只有在 [■ 入] 設定為 [True] 時，才能使用此設定。	✓
設定為桌布的 URL	字串		可讓您為登入畫面設定您選擇的桌布。若要使用此設定，請輸入您要為登入螢幕背景圖樣設定的影像 URL。此影像可能不同於使用 [■] ■ 設定的 [受控主畫面] 背景布。只有在 [■ 入] 設定為 [True] 時，才能使用此設定。	✓

項目名稱	資料類型	預設值	說明	驗證結果
在登入頁面上啟用顯示組織標誌	bool	TRUE	將此設定轉換為 True, 以使用將會出現在登入畫面和會話 PIN 畫面上的公司標誌。此設定會與 裝置鎖定 搭配使用, 而且只有在 [裝置鎖定 入] 設定為 [True] 時才能使用。	✓
登入頁面上的組織標誌	字串		可讓您在受控主畫面登入畫面和會話 PIN 畫面上, 以您選擇的標誌為裝置加上商標。若要使用此設定, 請輸入您要為標誌設定的影像 URL。只有在 [裝置鎖定] 和 [裝置鎖定 入] 設定為 [True] 時, 才能使用此設定。	✓
啟用會話 PIN	bool	假	如果您希望終端使用者成功登入受控主畫面之後, 收到建立本機會話 PIN 的提示, 請將此設定轉換為 True。會話 PIN 提示會在使用者取得主畫面的存取權之前出現, 並可與其他功能搭配使用。會話 PIN 會在使用者登入期間持續, 並在登出時清除。根據預設, 此設定已關閉。只有在 [裝置鎖定 入] 設定為 [True] 時, 才能使用此設定。	✓

類別	項目	說明	設定	備註
會話 PIN 的複雜度	字串		選擇本機會話 PIN 應該 []、[] 或 []。如果您選擇 []，使用者只需要輸入數值 PIN。如果您選擇 []，系統會提示使用者建立具有英數位元字元的 PIN，且不允許重複 (444) 或已排序的序列 (123、432、246)。重複和循序模式的評估會從三 (3) 位數/字元開始。如果您選擇 []，則系統會提示使用者使用英數位元建立 PIN，而且至少需要一個符號或字母。不允許 (123、432、246) 重複 (444) 或已排序的序列。重複和循序模式的評估會從三 (3) 個字元開始。此設定的預設值是一個 (1)，其中一個 (1) 表示使用者在其會話 PIN 中必須至少有一個字元。只有在 [] [] PIN] 和 [] 入] 設定為 [True] 時，才能使用此設定。	✓ 注意：現在只有應用程式設定才能使用 [] 選項。
會話 PIN 的最小長度	字串		定義使用者會話 PIN 必須遵守的最小長度。這可以與會話 PIN 的任何複雜度值搭配使用。只有在 [] [] PIN] 和 [] 入] 設定為 [True] 時，才能使用此設定。	✗
會話 PIN 的嘗試次數上限	字串		定義使用者在自動從受控主畫面登出之前，可以嘗試輸入其會話 PIN 的最大次數。預設值為零 (0)，其中零 (0) 表示使用者會進行無限的嘗試。這可以與會話 PIN 的任何複雜度值搭配使用。只有在 [] [] PIN] 和 [] 入] 設定為 [True] 時，才能使用此設定。	✗

類別	類型	預設值	說明	驗證結果
客戶對應資料夾	布林值	假	使用此規格搭配建立受控 裝置 ，以建立無法在使用者輸入其會話 PIN 的情況下結束的資料夾。只有在 [裝置 PIN] 和 [裝置 入] 設定為 [True] 時，才能使用此設定。	✗
從螢幕保護裝置程式傳回後需要 PIN 碼	bool	假	如果您想要在螢幕保護裝置程式出現之後，要求使用者輸入其會話 PIN，以在 Managed Home Screen 上繼續活動，請將此設定設為 True。只有在 [裝置 入] 設定為 [True] 時，才能使用此設定。	✓
啟用自動登出	bool	假	將此設定轉換為 True，以在指定的閒置期間後自動將目前的使用者登出受控主畫面。與 Azure AD 共用裝置模式搭配使用時，使用者也會登出裝置上參與 Azure AD 共用裝置模式的所有應用程式。根據預設，此設定處於關閉狀態。只有在 [裝置 入] 設定為 [True] 時，才能使用此設定。	✓
自動登出時間	整數	300	設定在使用者自動登出受控主畫面之前，可在數秒內通過的閒置期間。只有在 [裝置 入] 和 [裝置 入] 設定為 [True] 時，才能使用此設定。	✓
計算自動登出對話方塊的停機時間	整數	60	在使用者登出 Managed Home Screen 之前通知使用者的時間量，以秒為單位。只有在 [裝置 入] 和 [裝置 入] 設定為 [True] 時，才能使用此設定。	✓

名稱	類型	說明	預設值
隱私權聲明標題	字串	選擇性地在 Microsoft 隱私權聲明旁的受控主畫面上顯示貴組織的自訂隱私權聲明。使用此設定來命名包含貴組織隱私權聲明的連結，這是在 隱私權聲明連結 中指定。	×
隱私權聲明連結	字串	選擇性地在 Microsoft 隱私權聲明旁的受控主畫面上顯示貴組織的自訂隱私權聲明。如果您設定連結但未設定 隱私權聲明標題 ，則標題會讀取「自訂隱私權聲明」。	×

輸入 JSON 資料

輸入 JSON 資料以設定受控主畫面的所有可用設定，以及在設定設計工具中停用的設定。

Configuration settings format ⓘ ▼

[Download JSON template](#)

```
1 {
2   "kind": "androidenterprise#managedConfiguration",
3   "productId": "com.microsoft.launcher.enterprise",
4   "managedProperty": [
5     {
6       "key": "grid_size",
7       "valueString": "Auto"
8     },
9   ]
}
```

除了上述) 上 (組態設計工具 資料表中 所列的可設定設定清單之外，下表還提供您只能透過 JSON 資料設定的組態金鑰。

名稱	類型	說明	預設值
設定允許列出的應用程式	bundleArray	<pre>{ "key": "applications", "valueBundleArray": [{ "managedProperty": [{ "key": "package", "valueString": "STRING_VALUE" }] }] }</pre>	可讓您從裝置上安裝的所有應用程式，定義一組可在主畫面上顯示的應用程式。您可以輸入要顯示之應用程式的應用程式套件名稱來定義應用程式。例如， <code>com.android.settings</code> 會讓設定可在主畫面上存取。您在本節中允許列出的應用程式應該已安裝在裝置上，才能顯示在主畫面上。

項目	項目	項目	項目
設定釘選的 Web 連結	bundleArray	<pre>{ "key": "weblinks", "valueBundleArray": [{ "managedProperty": [{ "key": "link", "valueString": STRING_VALUE }, { "key": "label", "valueString": STRING_VALUE }] }] }</pre>	可讓您將網站釘選為主畫面上的快速啟動圖示。使用此設定，您可以定義 URL，並將其新增至主畫面，讓終端使用者在瀏覽器中單次點選即可啟動。注意：建議您建立、指派及核准裝置的 受控 Google Play Web 連結 。當您這麼做時，它們會被視為允許列出的應用程式。
建立用於群組應用程式的受控資料夾	bundleArray	<pre>{ "key": "managed_folders", "valueBundleArray": [{ "managedProperty": [{ "key": "folder_name", "valueString": STRING_VALUE }, { "key": "content", "valueBundleArray": [{ "managedProperty": [{ "key": "type", "valueString": STRING_VALUE }, { "key": "label", "valueString": STRING_VALUE }, { "key": "package", "valueString": STRING_VALUE }, { "key": "class", "valueString": STRING_VALUE }, { "key": "link", "valueString": STRING_VALUE }] }] }] }] }</pre>	可讓您在這些資料夾內建立及命名資料夾和群組應用程式。終端使用者無法移動資料夾、重新命名資料夾，或移動資料夾內的應用程式。資料夾會以建立的順序出現，而資料夾內的應用程式會依字母順序顯示。注意：您想要群組到資料夾中的所有應用程式都必須視需要指派給裝置，而且必須已新增至受控主畫面。

下列語法是包含所有可用組態金鑰的範例 JSON 腳本：

```
{
  "kind": "androidenterprise#managedConfiguration",
  "productId": "app:com.microsoft.launcher.enterprise",
  "managedProperty": [
    {
      "key": "lock_home_screen",
      "valueBool": true
    },
    {
      "key": "wallpaper",
      "valueString": "default"
    },
    {
      "key": "icon_size",
      "valueInteger": 2
    },
    {
      "key": "app_folder_icon",
      "valueInteger": 0
    },
    {
      "key": "screen_orientation",
      "valueInteger": 1
    },
    {
      "key": "applications",
      "valueBundleArray": [
        {
          "managedProperty": [
            {
              "key": "package",
              "valueString": "app package name here"
```



```

    }
  ]
}
],
{
  "key": "weblinks",
  "valueBundleArray": [
    {
      "managedProperty": [
        {
          "key": "link",
          "valueString": "link here"
        },
        {
          "key": "label",
          "valueString": "weblink label here"
        }
      ]
    }
  ]
},
{
  "key": "widgets",
  "valueBundleArray": [
    {
      "managedProperty": [
        {
          "key": "package",
          "valueString": "package name of application that exposes the widget here. An
example: com.microsoft.launcher.enterprise"
        },
        {
          "key": "widget_class",
          "valueString": "class name of widget here. an example: Time"
        },
        {
          "key": "span_x",
          "valueInteger": 5
        },
        {
          "key": "span_y",
          "valueInteger": 2
        }
      ]
    }
  ]
},
{
  "key": "show_virtual_home",
  "valueBool": false
},
{
  "key": "virtual_home_type",
  "valueString": "swipe_up"
},
{
  "key": "show_virtual_status_bar",
  "valueBool": true
},
{
  "key": "exit_lock_task_mode_code",
  "valueString": "123456"
},
{
  "key": "show_wifi_setting",
  "valueBool": false
},
{

```

```

        "key": "show_bluetooth_setting",
        "valueBool": false
    },
    {
        "key": "show_flashlight_setting",
        "valueBool": false
    },
    {
        "key": "show_volume_setting",
        "valueBool": false
    },
    {
        "key": "show_device_info_setting",
        "valueBool": false
    },
    {
        "key": "show_device_name",
        "valueBool": false
    },
    {
        "key": "device_name",
        "valueString": "{{DeviceName}}"
    },
    {
        "key": "device_serial_number",
        "valueString": "{{SerialNumber}}"
    },
    {
        "key": "show_managed_setting",
        "valueBool": false
    },
    {
        "key": "enable_easy_access_debugmenu",
        "valueBool": false
    },
    {
        "key": "enable_wifi_allowlist",
        "valueBool": false
    },
    {
        "key": "wifi_allowlist",
        "valueBundleArray": [
            {
                "managedProperty": [
                    {
                        "key": "SSID",
                        "valueString": "name of Wi-Fi network 1 here"
                    }
                ]
            },
            {
                "managedProperty": [
                    {
                        "key": "SSID",
                        "valueString": "name of Wi-Fi network 2 here"
                    }
                ]
            }
        ]
    },
    {
        "key": "grid_size",
        "valueString": "4;5"
    },
    {
        "key": "app_order_enabled",
        "valueBool": true
    },
    {

```

```

    "key": "apps_in_folder_ordered_by_name",
    "valueBool": true
  },
  {
    "key": "app_orders",
    "valueBundleArray": [
      {
        "managedProperty": [
          {
            "key": "package",
            "valueString": "com.Microsoft.emmx"
          },
          {
            "key": "type",
            "valueString": "application"
          },
          {
            "key": "container",
            "valueInteger": 1
          },
          {
            "key": "position",
            "valueInteger": 1
          }
        ]
      },
      {
        "managedProperty": [
          {
            "key": "folder_name",
            "valueString": "Work"
          },
          {
            "key": "type",
            "valueString": "managed_folder"
          },
          {
            "key": "container",
            "valueInteger": 1
          },
          {
            "key": "position",
            "valueInteger": 2
          }
        ]
      },
      {
        "managedProperty": [
          {
            "key": "package",
            "valueString": "com.microsoft.launcher.enterprise"
          },
          {
            "key": "type",
            "valueString": "application"
          },
          {
            "key": "class",
            "valueString": "com.microsoft.launcher.launcher"
          },
          {
            "key": "container",
            "valueInteger": 1
          },
          {
            "key": "position",
            "valueInteger": 3
          }
        ]
      }
    ]
  }
]

```

```

    },
    {
        "managedProperty": [
            {
                "key": "package",
                "valueString": "class name for widget here"
            },
            {
                "key": "type",
                "valueString": "widget"
            },
            {
                "key": "container",
                "valueInteger": 1
            },
            {
                "key": "position",
                "valueInteger": 1
            }
        ]
    }
]
},
{
    "key": "managed_folders",
    "valueBundleArray": [
        {
            "managedProperty": [
                {
                    "key": "folder_name",
                    "valueString": "Folder name here"
                },
                {
                    "key": "applications",
                    "valueBundleArray": [
                        {
                            "managedProperty": [
                                {
                                    "key": "package",
                                    "valueString": "com.microsoft.emmx"
                                }
                            ]
                        },
                        {
                            "managedProperty": [
                                {
                                    "key": "package",
                                    "valueString": "com.microsoft.bing"
                                }
                            ]
                        },
                        {
                            "managedProperty": [
                                {
                                    "key": "link",
                                    "valueString": "https://microsoft.com/"
                                }
                            ]
                        }
                    ]
                }
            ]
        }
    ]
},
{
    "managedProperty": [
        {
            "key": "folder_name",
            "valueString": "Example folder name 2"
        }
    ]
}

```

```

        },
        {
            "key": "is_customer_facing",
            "valueBool": true
        },
        {
            "key": "applications",
            "valueBundleArray": [
                {
                    "managedProperty": [
                        {
                            "key": "package",
                            "valueString": "com.microsoft.office.word"
                        }
                    ]
                }
            ]
        }
    ]
}

},
{
    "key": "show_notification_badge",
    "valueBool": true
},
{
    "key": "show_screen_saver",
    "valueBool": true
},
{
    "key": "screen_saver_image",
    "valueString": "URL to desired screen saver image here"
},
{
    "key": "screen_saver_show_time",
    "valueInteger": 0
},
{
    "key": "inactive_time_to_show_screen_saver",
    "valueInteger": 30
},
{
    "key": "media_detect_before_screen_saver",
    "valueBool": true
},
{
    "key": "enable_max_inactive_time_outside_MHS",
    "valueBool": false
},
{
    "key": "enable_max_absolute_time_outside_MHS",
    "valueBool": false
},
{
    "key": "max_inactive_time_outside_MHS",
    "valueInteger": 180
},
{
    "key": "max_absolute_time_outside_MHS",
    "valueInteger": 600
},
{
    "key": "theme_color",
    "valueString": "light"
},
{
    "key": "enable_mhs_signin",
    "valueBool": true
},

```

```

    },
    {
        "key": "signin_type",
        "valueString": "AAD"
    },
    {
        "key": "signin_screen_wallpaper",
        "valueString": "URL to desired image for signin screen wallpaper here"
    },
    {
        "key": "enable_corporate_logo",
        "valueBool": true
    },
    {
        "key": "signin_screen_branding_logo",
        "valueString": "URL to desired image for branding logo here"
    },
    {
        "key": "enable_session_PIN",
        "valueBool": true
    },
    {
        "key": "session_PIN_complexity",
        "valueString": "simple"
    },
    {
        "key": "max_number_of_attempts_for_session_PIN",
        "valueInteger": 0
    },
    {
        "key": "minimum_length_for_session_PIN",
        "valueInteger": 1
    },
    {
        "key": "max_number_of_attempts_for_exit_PIN",
        "valueInteger": 0
    },
    {
        "key": "amount_of_time_before_try_exit_PIN_again",
        "valueInteger": 0
    },
    {
        "key": "enable_auto_signout",
        "valueBool": true
    },
    {
        "key": "inactive_time_to_signout",
        "valueInteger": 300
    },
    {
        "key": "auto_signout_time_to_give_user_notice",
        "valueInteger": 30
    },
    {
        "key": "enable_PIN_to_resume",
        "valueBool": true
    },
    {
        "key": "custom_privacy_statement_title",
        "valueString": "name of custom privacy statement here"
    },
    {
        "key": "custom_privacy_statement_url",
        "valueString": "link to custom privacy statement here"
    },
    ],
}

```

Managed Home Screen 偵錯畫面

您可以選取 [上一頁] 按鈕來存取受控主畫面的偵錯畫面，直到偵錯畫面顯示 (選取 [上一頁] 按鈕 15 次或多次)。在此偵錯畫面中，您可以啟動 Android 裝置原則應用程式、檢視和上傳記錄，或暫時暫停 kiosk 模式以更新裝置。如需暫停 kiosk 模式的詳細資訊，請參閱 Android 中的 **離開 kiosk 模式** 專案Enterprise [專用裝置設定](#)。如果您想要更輕鬆的方式來存取受控主畫面的偵錯畫面，您可以使用裝置設定原則啟用 [快速存取偵錯] 功能表設定，也可以使用應用程式設定原則將 [啟用輕鬆存取偵錯] 功能表設定為 `True`。

後續步驟

- 如需 Android Enterprise專用裝置的詳細資訊，請參閱[設定 Android Enterprise專用裝置的Intune註冊](#)。

如何設定Intune 公司入口網站應用程式、公司入口網站網站和Intune應用程式

2022/9/27 •

公司入口網站應用程式、公司入口網站網站和 Android 上的Intune應用程式是使用者存取公司資料並可執行一般工作的位置。一般工作可能包括註冊裝置、安裝應用程式，以及尋找資訊 (例如 IT 部門) 的協助。此外，他們允許使用者安全地存取公司資源。使用者體驗提供數個不同的頁面，例如首頁、應用程式、應用程式詳細資料、裝置和裝置詳細資料。若要在公司入口網站內快速尋找應用程式，您可以在 [應用程式] 頁面上篩選應用程式。

NOTE

公司入口網站支援Configuration Manager應用程式。這項功能可讓終端使用者在共同管理的客戶公司入口網站中看到Configuration Manager和Intune部署的應用程式。這個新版本的公司入口網站會為所有共同管理的客戶顯示Configuration Manager部署的應用程式。這項支援可協助系統管理員合併其不同的使用者入口網站體驗。如需詳細資訊，請參閱[在共同管理的裝置上使用公司入口網站應用程式](#)。

iOS 公司入口網站 應用程式的最低支援版本是 v4.16.0。如果使用者執行 v4.14.1 或以下版本，系統會在登入時提示他們更新。

自訂使用者體驗

藉由自訂使用者體驗，您將協助為終端使用者提供熟悉且實用的體驗。若要這樣做，請流覽至 [Microsoft 端點管理員 系統管理中心](#)，然後選取 [租使用者系統管理 > 自訂]，您可以在其中編輯預設原則，或建立最多 10 個群組目標原則。這些設定會套用至 Android 上的公司入口網站應用程式、公司入口網站網站和Intune應用程式。

商標

下表提供使用者體驗的品牌自訂詳細資料：

圖示	說明
	此名稱會在使用者體驗的整個訊息中顯示。它可以設定為顯示在標頭中，以及使用 [圖示] 設定。最大長度為 40 個字元。
Color	選擇 [圖示] 可從五種標準色彩中選擇。選擇 [圖示] 以根據十六進位代碼值選取特定色彩。
	設定要在使用者體驗中顯示的主題色彩。我們會自動將文字色彩設定為黑色或白色，使其最能在您選取的主題色彩上顯示。
	選取終端使用者體驗中的標頭是否應顯示  、  或  。下列預覽方塊只會顯示標誌，而不會顯示名稱。
	上傳您想要在所選主題色彩上顯示的標誌。為了獲得最佳外觀，請上傳具有透明背景的標誌。您可以在設定下方的預覽方塊中查看其外觀。 建議的影像高度：大於 72 px 檔案大小上限：750KB 檔案類型：PNG、JPG 或 JPEG

	
	上傳您想要在白色或淺色背景上顯示的標誌。為了獲得最佳外觀，請上傳具有透明背景的標誌。您可以在設定下方的預覽方塊中，查看其在白色背景的外觀。 建議的影像高度：大於 72 px 檔案大小上限：750KB 檔案類型：PNG、JPG 或 JPEG
	上傳反映貴組織品牌的影像。 - 建議的影像寬度：大於 1125 圖元 - 影像大小上限：1.3 MB - 檔案類型：PNG、JPG 或 JPEG - 它會顯示在下列位置： - iOS/iPadOS 公司入口網站：使用者設定檔頁面上的背景影像。 - Windows 公司入口網站：使用者設定檔頁面上的背景影像。 - 公司入口網站網站：使用者設定檔頁面上的背景影像。 - Android Intune應用程式：在隱藏式選單中，並作為使用者設定檔頁面上的背景影像。

NOTE

當使用者從公司入口網站安裝 iOS/iPadOS 應用程式時，他們會收到提示。當 iOS/iPadOS 應用程式連結至應用程式市集、連結至大量採購方案 (VPP)，或連結至企業營運 (LOB) 應用程式時，就會發生這種情況。提示可讓使用者接受動作或允許管理應用程式。提示會顯示您的公司名稱，或當您的公司名稱無法使用時，。

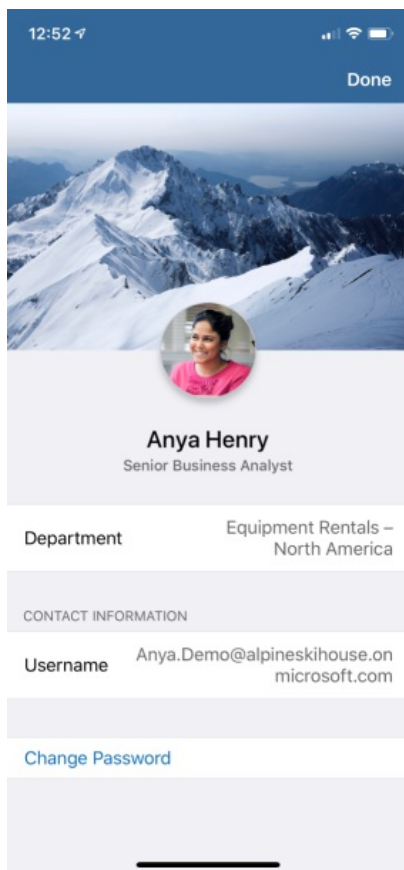
品牌影像最佳做法

正確的品牌映射可藉由展現貴組織品牌的強感，來增強使用者的信任。以下是您可能想要考慮的一些秘訣，以取得、選擇及優化顯示位置的影像。

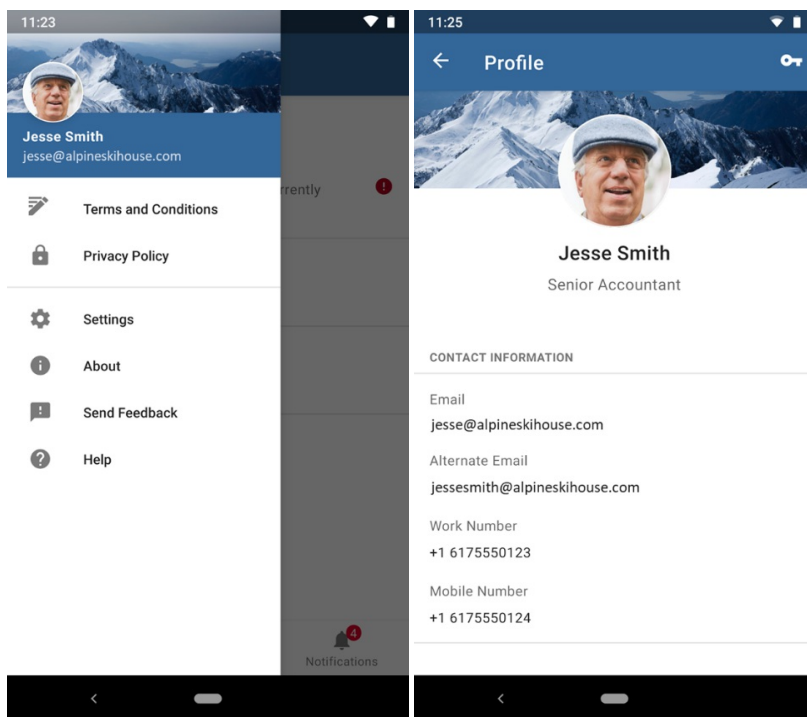
- 與您的行銷或藝術部門聯繫。它們可能已經有一組已核准的品牌映射。它們也可以協助您視需要優化映射。
- 請考慮橫向和直向組合。影像應該有足夠的背景圍繞著焦點。根據裝置大小、方向和平臺，影像可能會以不同的方式裁剪。
- 避免使用泛型股票映射。此影像應該會反映貴組織的品牌，並讓使用者感到熟悉。如果您沒有帳戶，最好不要使用一個，而不是使用對您的使用者沒有任何意義的泛型。
- 移除不必要的中繼資料。影像檔可以隨附中繼資料，例如相機設定檔、地理位置、標題、標題等等。使用影像優化工具來去除這項資訊，以在符合檔案大小限制時維持品質。

品牌影像範例

下圖顯示 iPhone 上的品牌影像範例：



以下顯示 Android Intune 應用程式中的品牌影像範例：



支援資訊

輸入貴組織的支援資訊，讓員工可以提出問題。此支援資訊會顯示在使用者體驗的支援、說明&支援和技術服務人員頁面上。

連絡人名稱	40	此名稱是使用者連絡支援人員時會聯繫的人員。

欄位	長度	說明
電話號碼	20	此號碼可讓使用者呼叫 以尋求支援。
電子郵件地址	40	此電子郵件地址是使用者可以傳送電子郵件以取得支援的地方。您必須以 格式 <code>alias@domainname.com</code> 輸入有效的電子郵件地址。
網站名稱	40	這是在支援網站 URL 的某些位置中顯示的易記名稱。如果您指定支援網站 URL 且沒有易記名稱, 則 URL 本身會顯示在使用者體驗中。
網站 URL	150	使用者應該使用的支援網站。URL 的格式 <code>https://www.contoso.com</code> 必須是。
其他資訊	120	在此包含任何其他與支援相關的傳訊給使用者。

組態

您可以特別針對註冊、隱私權、通知、應用程式來源和自助動作設定公司入口網站體驗。

註冊

下表提供註冊特定的設定詳細資料：

欄位	長度	說明
裝置註冊	不適用	指定是否應提示使用者註冊行動裝置管理。如需詳細資訊, 請參閱 裝置註冊設定選項 。

裝置註冊設定選項

若要支援裝置註冊設定, 終端使用者必須具備下列公司入口網站版本：

- iOS/iPadOS 上的公司入口網站:4.4 版或更新版本
- Android 上的公司入口網站:5.0.4715.0 版或更新版本

IMPORTANT

下列設定不適用於設定為使用 [自動裝置註冊註冊](#)的iOS/iPadOS 裝置。不論如何設定這些設定, 設定為使用自動裝置註冊註冊的 iOS/iPadOS 裝置都會在現成的流程期間註冊, 且使用者在啟動公司入口網站時會收到登入提示。

下列設定確實適用於使用 [Samsung Knox Mobile Enrollment \(KME\)](#) 設定的 Android 裝置。如果裝置已設定 KME, 且裝置註冊設定為 [無法使用], 則裝置將無法在現成流程期間註冊。

針對 Android 公司入口網站應用程式, 如果Intune偵測到使用者的裝置已針對[應用程式保護](#)原則進行設定, 而不需註冊, 即使裝置註冊設定已設定為提示註冊, 也不會提示使用者註冊公司入口網站。這適用於 Surface Duo 裝置以外的所有 Android 裝置類型。

欄位	長度	欄位	長度	欄位	長度

狀態	說明	是否	是否	是否	是否 (如果適用)
可用, 具有提示	提示在所有可能的位置註冊的預設體驗。	是	是	是	是
可用, 沒有提示	使用者可以透過目前裝置的裝置詳細資料狀態, 或從需要註冊的應用程式註冊。	否	否	是	是
無法	使用者無法註冊。需要註冊的應用程式將會隱藏。	否	否	否	否

隱私權

下表提供隱私權特定的設定詳細資料：

設定	設定 ID	說明
隱私權聲明 URL	79	將貴組織的隱私權聲明設定為在使用者按一下隱私權連結時顯示。您必須以格式 <code>https://www.contoso.com</code> 輸入有效的 URL。這是必要欄位。
iOS/iPadOS (無法查看或執行哪些支援的隱私權訊息)	520	保留預設訊息或自訂訊息, 以列出貴組織在受控 iOS/iPadOS 裝置上看不到的專案。您可以使用 Markdown 來新增專案符號、粗體、斜體和連結。
iOS/iPadOS 可查看或執行哪些支援 (隱私權訊息)	520	保留預設訊息或自訂訊息, 以列出貴組織可在受控 iOS/iPadOS 裝置上看到的專案。您可以使用 Markdown 來新增專案符號、粗體、斜體和連結。

如需相關資訊, [請參閱設定公司入口網站和Microsoft Intune應用程式的意見反應設定。](#)

應用程式來源

您可以選擇要在公司入口網站中顯示哪些其他應用程式來源。

NOTE

公司入口網站支援Configuration Manager應用程式。這項功能可讓終端使用者在共同管理的客戶公司入口網站中看到Configuration Manager和Intune部署的應用程式。如需詳細資訊, [請參閱在共同管理的裝置上使用公司入口網站應用程式。](#)

下表提供應用程式來源的特定設定詳細資料：

設定	設定 ID	說明
Azure AD 企業應用程式	不適用	選 ☐ 或 ☐ 以在每個使用者的公司入口網站中顯示 Azure AD Enterprise 應用程式。如需詳細資訊, 請參閱 應用程式來源設定選項 。

類別	類別	類別
Office Online 應用程式	不適用	選 ☐ [■] 或 ☐ [■] 以在每個使用者的公司入口網站中顯示 Office Online 應用程式。如需詳細資訊，請參閱 應用程式來源設定選項 。

應用程式來源設定選項

NOTE

只有 Windows 公司入口網站 和 公司入口網站 網站才支援顯示來自其他 Microsoft 服務的應用程式。

您可以在每個使用者的公司入口網站中隱藏或顯示 Azure AD Enterprise 應用程式 和 Office Online 應用程式。顯示 會導致公司入口網站顯示所選 Microsoft 服務的整個應用程式目錄，(指派給使用者的)。Azure AD Enterprise 應用程式 會透過 [Microsoft 端點管理員 系統管理中心](#) 進行註冊和指派。Office Online 應用程式 會使用 [M365 管理員中心](#) 提供的授權控制來指派。在 [Microsoft 端點管理員 系統管理中心](#)，選取 [\[租使用者系統管理 > 自訂\]](#) 以尋找此組態設定。根據預設，每個額外的應用程式來源都會設定為 [\[隱藏\]](#)。

自訂移除和重設裝置動作

您可以針對 Windows 和 iOS 裝置自訂 [移除](#) 和 [重設](#) 自助裝置動作的可見度，這些動作會在 公司入口網站 應用程式、公司入口網站 網站及 Android 上的 Intune 應用程式中，跨平臺向終端使用者顯示。若要防止使用者移除或重設公司 Windows 和 iOS 裝置，您可以在 [租使用者管理 > 自訂](#) 中隱藏這些動作。

您可以使用下列動作：

- 在公司 Windows 裝置上隱藏 [\[移除\]](#) 按鈕。(此設定一律會顯示為已停用，因為公司 Windows 裝置的 [\[移除\]](#) 按鈕一律會隱藏。)
- 在公司 Windows 裝置上隱藏 [\[重設\]](#) 按鈕。
- 在公司 iOS/iPadOS 裝置上隱藏 [\[移除\]](#) 按鈕。
- 在公司 iOS/iPadOS 裝置上隱藏 [\[重設\]](#) 按鈕。

NOTE

這些動作可用來限制公司入口網站應用程式和網站中的裝置動作，而不會實作任何裝置限制原則。若要限制使用者執行原廠重設或從設定移除 MDM，您必須設定裝置限制原則。

此外，這些自訂專案僅適用於預設的自訂原則，而非以自訂原則為目標的群組。

公司入口網站網站中的裝置合規性狀態

終端使用者可以從公司入口網站網站查看其裝置的合規性狀態。終端使用者可以流覽至 [公司入口網站](#) 網站，然後選取 [\[裝置\]](#) 頁面以查看裝置狀態。裝置的狀態會是 [\[可以存取公司資源\]](#)、[\[檢查存取權\]](#) 或 [\[無法存取公司資源\]](#)。如需相關資訊，請參閱從 [公司入口網站 網站管理應用程式](#)。

開啟 Web 公司入口網站 應用程式

針對 Web 公司入口網站 應用程式，如果終端使用者已安裝公司入口網站應用程式，終端使用者會看到對話方塊，詢問使用者在瀏覽器外部開啟時要如何開啟應用程式。如果應用程式不在公司入口網站的路徑中，則公司入口網站會開啟首頁。如果應用程式位於路徑中，則公司入口網站會開啟特定應用程式。

選取公司入口網站時，當 URI 路徑為下列其中一個時，系統會將使用者導向至應用程式中的對應頁面：

- `/apps` - Web 公司入口網站會開啟列出所有應用程式的 [\[應用程式\]](#) 頁面。
- `/apps/[appID]` - Web 公司入口網站會開啟對應應用程式的 [\[詳細資料\]](#) 頁面。
- *URI 路徑不同或非預期* - 將會顯示網頁公司入口網站首頁。

如果使用者未安裝公司入口網站應用程式，使用者將會進入 Web 公司入口網站。

NOTE

為了改善公司入口網站網站上的頁面載入效能，應用程式圖示現在會分批載入。使用者在載入公司入口網站網站時，可能會暫時看到其部分應用程式的預留位置圖示。

如需意見反應相關資訊，請參閱[設定公司入口網站](#)和[Microsoft Intune 應用程式的意見反應設定](#)。

適用於 iOS/iPadOS 的公司入口網站 和 Apple 設定助理

針對執行 13.0 和更新版本的 iOS/iPadOS 裝置，在建立自動化裝置註冊設定檔時，您現在可以選擇新的驗證方法：**使用新式驗證設定 助理**。這個方法提供所有安全性，使其無法向公司入口網站進行驗證，但可避免讓終端使用者停滯在裝置上，而在裝置上安裝公司入口網站時無法使用的問題。使用者必須使用 Azure AD 認證在設定助理畫面期間進行驗證。這需要在公司入口網站應用程式中進行額外的 Azure AD 登入後註冊，才能存取受條件式存取保護的公司資源，以及 Intune 來評估裝置合規性。正確的公司入口網站版本會自動傳送為 iOS/iPadOS 裝置的必要應用程式，建議您從註冊設定檔中選擇的 VPP 權杖。

註冊會在使用者登陸主畫面後完成，而且使用者可以自由地針對不受條件式存取保護的資源使用裝置。當使用者完成額外的 Azure AD 登入裝置上的公司入口網站應用程式時，就會建立使用者親和性。如果租使用者已針對這些裝置或使用者開啟多重重要素驗證，系統會要求使用者在安裝助理期間完成多重重要素驗證。不需要多重重要素驗證，但可視需要在條件式存取內使用此驗證方法。

公司入口網站 iOS/iPadOS 裝置的衍生認證

Intune 與認證提供者 DISA Purebred、Entrust 和 Intercede 合作，支援個人身分識別驗證 (PIV) 和 Common Access Card (CAC) 衍生認證。使用者會在註冊其 iOS/iPadOS 裝置之後進行其他步驟，以在公司入口網站應用程式中驗證其身分識別。系統會先為您的租使用者設定認證提供者，然後將使用衍生認證的設定檔設為使用者或裝置，為使用者啟用衍生認證。

NOTE

使用者會根據您透過 Intune 指定的連結，看到衍生認證的相關指示。

如需 iOS/iPadOS 裝置之衍生認證的詳細資訊，請參閱在 [Microsoft Intune 中使用衍生認證](#)。

公司入口網站的深色模式

深色模式適用於 iOS/iPadOS、macOS 和 Windows 公司入口網站。使用者可以下載應用程式、管理其裝置，以及根據裝置設定，在其選擇的色彩配置中取得 IT 支援。iOS/iPadOS、macOS 和 Windows 公司入口網站會自動符合使用者的深色或淺色模式裝置設定。

Windows 公司入口網站鍵盤快速鍵

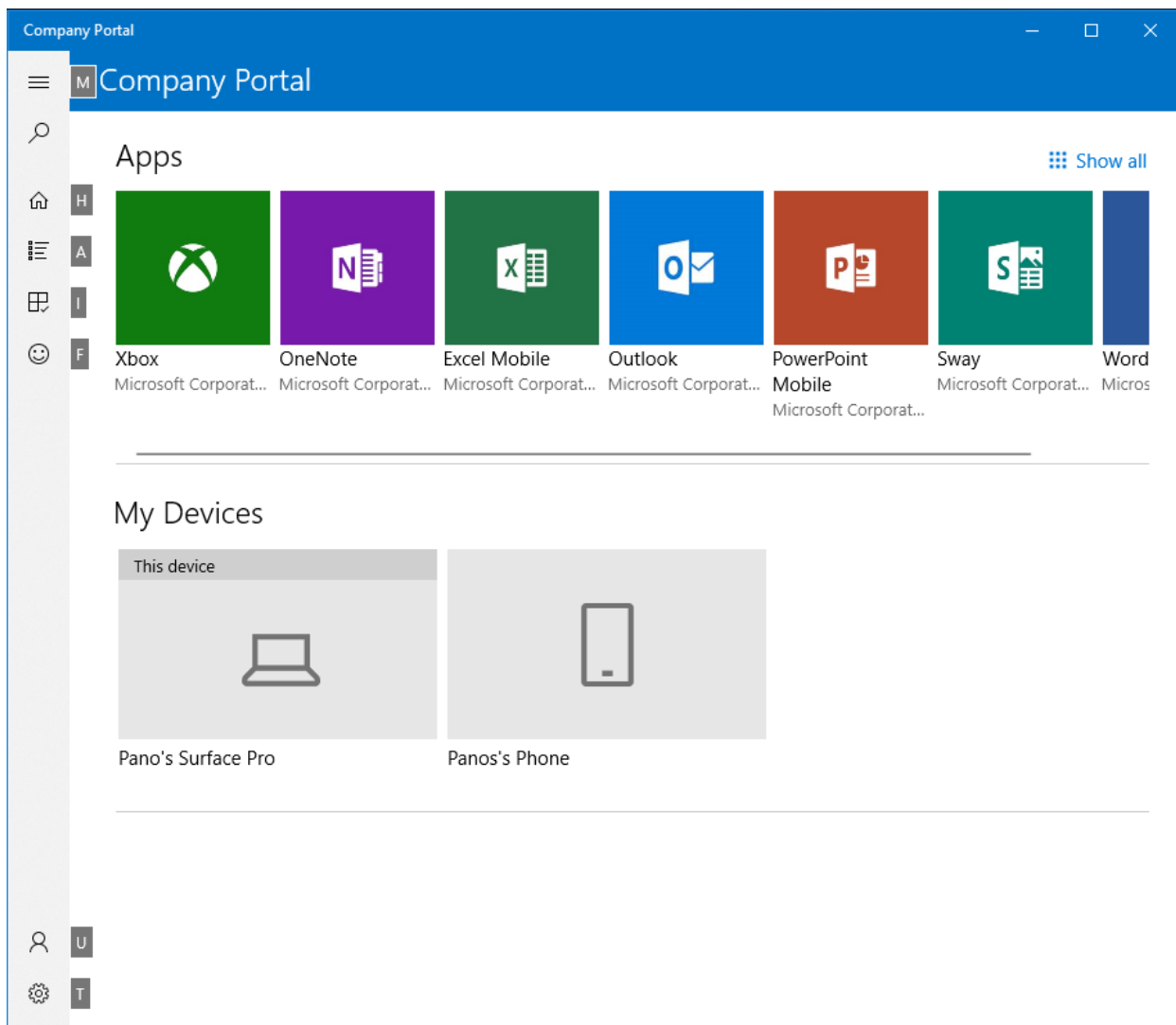
終端使用者可以使用鍵盤快速鍵 (快速鍵)，在 Windows 公司入口網站中觸發流覽、應用程式和裝置動作。

下列鍵盤快速鍵可在 Windows 公司入口網站 應用程式中使用。

⌘	⌘	⌘⌘⌘
導覽功能表	導覽	Alt+M
	首頁	Alt+H

☰	☰	☰☰☰
	所有應用程式	Alt+A
	所有裝置	Alt+D
	下載&更新	Alt+U
	傳送意見反應	Alt+F
	我的設定檔	Alt+P
	設定	Alt+T
裝置磚	重新命名	F2
	移除	Ctrl+D 或 Delete
	檢查存取權	Ctrl+M 或 F9
裝置詳細資料	重新命名	F2
	移除	Ctrl+D 或 Delete
	檢查存取權	Ctrl+M 或 F9
應用程式詳細資料	安裝	Ctrl+I
應用程式清單磚	安裝	Ctrl+I
應用程式清單專案	安裝	Ctrl+I

終端使用者也可以在 Windows 公司入口網站 應用程式中看到可用的快捷方式。



來自公司入口網站的使用者自助裝置動作

使用者可以透過公司入口網站應用程式、公司入口網站網站或 Android 上的Intune應用程式，在其本機或遠端裝置上執行動作。使用者可以執行的動作會根據裝置平臺和設定而有所不同。在所有情況下，遠端裝置動作只能由裝置的主要使用者執行。

可用的自助裝置動作包括下列各項：

- **淘汰**– 從 Intune 管理中移除裝置。在公司入口網站應用程式和網站中，這會顯示為 **[移除]**。
- **抹除**– 此動作會起始裝置重設。在公司入口網站中，這會在 iOS/iPadOS 公司入口網站 應用程式中顯示為 **[重設]** 或 **[原廠 重設]**。
- **重新命名**– 此動作會變更使用者可在公司入口網站中看到的裝置名稱。它不會變更本機裝置名稱，只會變更公司入口網站中的清單。
- **同步 處理**– 此動作會起始與Intune服務的裝置簽入。這会在公司入口網站中顯示為 **[檢查狀態]**。
- **遠端鎖定**– 這會鎖定裝置，需要 PIN 才能解除鎖定。
- **重設密碼**– 此動作可用來重設裝置密碼。在 iOS/iPadOS 裝置上，將會移除密碼，而且使用者必須在設定中輸入新的程式碼。在支援的 Android 裝置上，Intune會產生新的密碼，並暫時顯示在公司入口網站中。
- **金鑰復原**– 此動作可用來從公司入口網站網站復原加密 macOS 裝置的個人修復金鑰。

若要自訂可用的使用者自助動作，請參閱[自訂公司入口網站的使用者自助動作](#)。

Self-Service動作

某些平臺和設定不允許自助式裝置動作。下表提供有關自助動作的進一步詳細資料：

II	WINDOWS 10 ⁽³⁾	IOS/IPADOS ⁽³⁾	MACOS ⁽³⁾	ANDROID ⁽³⁾
淘汰	(¹)	(⁹)	可以使用	(⁷)
擦去	可以使用	(⁵) (⁹)	NA	(⁷)
重新命名 ⁽⁴⁾	提供	提供	提供	提供
同步處理	提供	提供	提供	提供
金鑰復原	NA	NA	(²)	NA

⁽¹⁾已加入 Azure AD 的 Windows 裝置上一律會封鎖 **淘汰**。

⁽²⁾只能透過入口網站取得 macOS 的 **金鑰復原**。

⁽³⁾如果使用裝置註冊管理員註冊，則會停用所有遠端動作。

⁽⁴⁾**重新命名** 只會變更公司入口網站應用程式或入口網站中的裝置名稱，而不會變更裝置上的裝置名稱。

⁽⁵⁾**抹除** 無法在使用者註冊的 iOS/iPadOS 裝置上使用。

某些 Android 和 Android Enterprise 設定不支援 ⁽⁶⁾ **重設密碼**。如需詳細資訊，請參閱[重設或移除Intune中的裝置密碼](#)。

⁽⁷⁾**淘汰** 和 **抹除** 不適用於 Android Enterprise 裝置擁有者案例，(COPE、COBO、COSU)。

⁽⁸⁾使用者註冊的 iOS/iPadOS 裝置不支援 **重設密碼**。

⁽⁹⁾所有 iOS/iPadOS 自動化裝置註冊裝置 (先前稱為 DEP) 已停用 **[淘汰]** 和 **[抹除]** 選項。

應用程式記錄

如果您使用 Azure Government，應用程式記錄會提供給使用者，以決定使用者在起始程式以取得問題協助時的共用方式。不過，如果您不是使用 Azure Government，當使用者起始程式以取得問題的協助時，公司入口網站會將應用程式記錄直接傳送給 Microsoft。將應用程式記錄傳送至 Microsoft 可讓您更輕鬆地進行疑難排解和解決問題。

NOTE

與 Microsoft 和 Apple 原則一致，我們不會基於任何原因，將服務所收集的任何資料銷售給任何協力廠商。

公司入口網站代理程式更新

公司入口網站應用程式可以從 Microsoft 端點管理員 主控台儲存，以及顯示傳送給使用者裝置的推播通知。選擇接收公司入口網站推播通知的使用者，可以在公司入口網站的 **[通知]** 索引標籤中，檢視和管理您傳送給其裝置的自訂預存訊息。

NOTE

使用者必須更新為 Android 公司入口網站 (5.0.5291.0 版，發行于 2021 年 10 月，) 或 Android Intune app (2021.09.04 版，發行于 2021 年 9 月，) 在 Android 裝置上接收自訂通知。如果使用者未在 Intune 2111 年 11 月 (2111) 服務發行之前更新，而且會傳送自訂通知，則會改為收到通知，告知他們更新應用程式以檢視通知。更新應用程式之後，他們會在應用程式的 **[通知]** 區段中看到貴組織所傳送的訊息。

來自 iOS/iPadOS 公司入口網站 應用程式的通知現在會使用預設 Apple 音效傳遞至裝置，而不是以無訊息方式傳遞。若要從 iOS/iPadOS 公司入口網站 應用程式關閉通知音效，請選取 **[設定 > 通知 >]**[Comp Portal]，然後選取 **[音效]** 切換。

如需通知的詳細資訊，請參閱 [接收自訂通知](#)。

設定公司入口網站和Microsoft Intune應用程式的意見反應設定

有一些 M365 企業原則會影響目前記錄使用者的意見反應是否必須啟用或停用。這些原則可透過[Microsoft 365 Apps 系統管理中心](#)取得。相對於Microsoft Intune, 這些原則會影響Intune 公司入口網站應用程式、Web 公司入口網站 和Microsoft Intune應用程式的意見反應和問卷調查。

M365 意見反應原則包含下列原則：

原則	狀態	描述
允許在 Office 中使用連線體驗	啟用	控制用戶端是否可以使用連線體驗套件, 包括意見反應。
允許使用者將意見反應提交給 Microsoft	啟用	控制應用程式中的意見反應進入點。
允許使用者接收和回應來自 Microsoft 的產品內問卷	啟用	控制產品內的問卷提示。
允許使用者在將意見反應提交給 Microsoft 時包含螢幕擷取畫面和附件	已停用	控制使用者可決定提交與意見反應和問卷的中繼資料。
允許 Microsoft 追蹤使用者所提交的意見反應	已停用	控制使用者是否可以與意見反應和問卷共用連絡人資訊。
允許使用者在提交意見反應給 Microsoft 時包含記錄檔和內容範例	已停用	控制使用者可決定提交與意見反應和問卷的中繼資料。

若要設定意見反應原則設定：

- 移至[Microsoft 365 Apps系統管理中心](#)並登入。
- 選取 [自訂原則 > 管理 > 建立]。
- 輸入名稱和描述。
- 選擇將套用此原則的使用者類型。
- 為您的租使用者選擇將套用此原則的群組。
- 搜尋意見反應和問卷以尋找並選取原則。
- 針對列出的每個原則，將值設定為 [已啟用] 或 [已停用]。

後續步驟

- 在適用於 iOS 和 Android 的 Microsoft Edge 中設定新索引標籤頁面的組織標誌和品牌色彩
- 新增應用程式

設定 Microsoft Launcher

2022/9/27 •

Microsoft Launcher 是一個 Android 應用程式，可讓使用者個人化其手機、保持井然有序，以及從手機轉移到電腦。

在 Android Enterprise 完全受控裝置上，啟動器可讓企業 IT 系統管理員選取桌布、應用程式和圖示位置，來自訂受控裝置主畫面。這會標準化不同 OEM 裝置和系統版本上所有受控 Android 裝置的外觀與風格。

如何設定 Microsoft Launcher 應用程式

將 Microsoft Launcher 應用程式 [新增至Intune](#)之後，流覽至 [Microsoft 端點管理員 管理員 中心](#)，然後選取 [應用程式 > 應用程式設定原則]。為執行 Android 的受管理裝置 新增設定原則，然後選擇 [Microsoft Launcher] 作為相關聯的應用程式。按一下 [組態設定] 以設定不同的可用 Microsoft Launcher 設定。

選擇組態設定格式

有兩種方法可用來定義 Microsoft Launcher 的組態設定：

- 設定設計 工具可讓您使用容易使用的 UI 來設定設定，讓您開啟或關閉功能並設定值。在此方法中，有數個已停用且實數值型別為 BundleArray 的組態金鑰。這些設定金鑰只能藉由輸入 JSON 資料來設定。
- JSON 資料 可讓您使用 JSON 腳本定義所有可能的組態金鑰。

如果您 使用設定 設計工具新增屬性，您可以從 [組態 設定格式] 下拉式清單中選取 [輸入 JSON 資料]，自動將這些屬性轉換成 JSON，如下所示。

 Use the JSON editor to configure the disabled configuration keys.

Configuration settings format ⓘ

Use configuration designer

Use configuration designer

Enter JSON data

NOTE

透過設定設計工具設定屬性之後，JSON 資料也會更新，只反映這些屬性。若要將其他組態金鑰新增至 JSON 資料，請使用 [JSON 腳本範例](#) 來複製每個組態金鑰的必要行。

編輯先前建立的應用程式設定原則時，如果已設定複雜的屬性，編輯程式將會顯示 JSON 資料編輯器。所有先前設定的設定都會保留下來，而且您可以切換為使用組態設計工具來修改支援的設定。

使用設定設計工具

設定設計工具可讓您選取預先填入的設定及其相關聯的值。

 Use the JSON editor to configure the disabled configuration keys.

Configuration settings format ⓘ

Use configuration designer

Add

CONFIGURATION KEY	VALUE TYPE	CONFIGURATION VALUE	DESCRIPTION
Home Screen App Order Us...	bool	true	This key specifies whether the Hom...
Feed Enable User Change All...	bool	☒	This key specified whether the Fee...
Set Device Wallpaper User C...	bool	true	This key specifies whether the Set ...
Feed Enable	bool	true	This key specifies whether the feed ...
Set Device Wallpaper	string	Default	Allows you to set a wallpaper of yo...
Set Grid Size	string	Default	Allows you to set the grid size for a...
Enrollment Type	string	CorporateOwnedBusinessOnly	Indicates the device enrollment typ...

下表列出 Microsoft Launcher 可用的組態索引鍵、數值型別、預設值和描述。描述會根據選取的值提供預期的裝

置行為。在設定設計工具中停用的組態金鑰不會列在資料表中。

名稱	類型	預設	說明
註冊類型	字串	預設	可讓您設定此原則應套用的註冊類型。默認值目前是指 CorporateOwnedBusinessOnly。目前沒有其他支援的註冊類型。JSON 金鑰名稱: management_mode_key
允許主畫面應用程式訂單使用者變更	布林值	True	可讓您指定使用者是否可以變更 [設定裝置桌布] 設定。 - 如果設定為 True, 則只會針對初始部署強制執行原則中定義的應用程式順序。之後, 將不會強制執行原則, 以遵守使用者可能所做的任何變更。 - 如果設定為 False, 則會在每次同步處理時強制執行應用程式訂單。 ■: 主畫面應用程式訂單只能透過 JSON 編輯器來設定。 JSON 金鑰名稱: <pre>com.microsoft.launcher.HomeScreen.AppOrder.UserChar</pre>
設定格線大小	字串	自動	可讓您設定要在主畫面上放置應用程式的格線大小。您可以設定應用程式資料列和資料行的數目, 以下列格式定義格線大小: <pre>columns;rows</pre> 。如果您定義格線大小, 將顯示在主畫面上資料列中的應用程式數目上限會是您設定的資料列數目, 而將顯示在主畫面資料行中的應用程式數目上限會是您設定的資料行數目。 JSON 金鑰名稱: <pre>com.microsoft.launcher.HomeScreen.GridSize</pre>
設定裝置背景圖樣	字串	Null	可讓您輸入要設定為桌布的影像 URL, 以設定您選擇的背景圖樣。 JSON 金鑰名稱: <pre>com.microsoft.launcher.Wallpaper.URL</pre>
設定允許的裝置桌布使用者變更	布林值	True	可讓您指定使用者是否可以變更 [設定裝置桌布] 設定。 - 如果設定為 True, 則只會針對初始部署強制執行原則中的桌布。之後, 將不會強制執行原則, 以遵守使用者可能所做的任何變更。 - 如果設定為 False, 則會在每次同步處理時強制執行桌布。 JSON 金鑰名稱: <pre>com.microsoft.launcher.Wallpaper.URL.UserChangeAll</pre>

名稱	類型	預設值	說明
摘要啟用	布林值	True	可讓您在使用者在主畫面向右撥動時, 在裝置上啟用啟動器摘要。 - 如果設定為 True, 則會啟用摘要。 - 如果設定為 False, 則會停用摘要。 JSON 金鑰名稱: com.microsoft.launcher.Feed.Enabled
摘要啟用允許使用者變更	布林值	True	可讓您指定使用者是否可以變更 [摘要] 設定。 - 如果設定為 True, 則只會針對初始部署強制執行摘要。之後, 將不會強制執行原則, 以遵守使用者可能所做的任何變更。 - 如果設定為 False, 每次同步處理時都會強制執行摘要。 JSON 金鑰名稱: com.microsoft.launcher.Feed.Enabled.UserChangeAllow
搜尋列位置	字串	靠下	可讓您指定 [搜尋列] 主畫面上的位置。 - 如果設定為 [靠下], 搜尋列會位於主畫面底部。 - 如果設定為 [靠上], 搜尋列會位於主畫面頂端。 - 如果設定為 [隱藏], 搜尋列將會從主畫面中移除。 JSON 金鑰名稱: com.microsoft.launcher.Search.SearchBar.Placement
允許搜尋列放置使用者變更	布林值	True	可讓您指定使用者是否可以變更 [搜尋列] 設定。 - 如果設定為 True, 則只會針對初始部署強制執行搜尋列位置。之後, 將不會強制執行原則, 以遵守使用者可能所做的任何變更。 - 如果設定為 False, 則會在每次同步處理時強制執行搜尋列的位置。 JSON 金鑰名稱: com.microsoft.launcher.Search.SearchBar.Placement.AllowUserChange ■: 對於 Microsoft Launcher 6.2 版和更新版本, 將不再強制執行此設定。因此, 將此值設定為 True 不會有任何作用。您的終端使用者將無法自訂其裝置上搜尋列位置。

說明	類型	預設值	詳細資訊
停駐模式	字串	顯示	可讓您在使用者從主畫面底部向上撥動時，在裝置上啟用 Dock。 - 如果設定為 [■]，則會啟用停駐。 - 如果設定為 [■]，停駐會從主畫面隱藏，但使用者可以在需要時顯示它。 - 如果設定為 [■]，則停用停駐。 JSON 金鑰名稱： <code>com.microsoft.launcher.Dock.Mode</code>
允許停駐模式使用者變更	字串	True	可讓您指定終端使用者是否可以變更 [停駐模式] 設定。 - 如果設定為 True，則只會針對初始部署強制執行停駐模式設定。之後，將不會強制執行原則，以遵守使用者可能所做的任何變更。 - 如果設定為 False，則會在每次同步處理時強制執行停駐模式設定。 JSON 金鑰名稱： <code>com.microsoft.launcher.Dock.Mode.UserChangeAllowed</code>

輸入 JSON 資料

輸入 JSON 資料來設定 Microsoft Launcher 的所有可用設定，以及設定設計工具中停用的設定，如下所示。

 Use the JSON editor to configure the disabled configuration keys.

Configuration settings format ⓘ

[Download JSON template](#)

```
1 {
2   "kind": "androidenterprise#managedConfiguration",
3   "productId": "com.microsoft.launcher",
4   "managedProperty": [
5     {
6       "key": "management_mode_key",
7       "valueString": "Default"
8     },
9     {
10      "key": "com.microsoft.launcher.Wallpaper.Url.UserChangeAllowed",
11      "valueBool": true
12    },
13    {
14      "key": "com.microsoft.launcher.Wallpaper.Url",
15      "valueString": "Default"
16    },
17    {
18      "key": "com.microsoft.launcher.Feed.Enable",
19      "valueBool": true
20    }
21  ]
22 }
```

除了上 上 (組態設計工具資料表中所列的可設定設定清單之外，下表還提供您只能透過 JSON 資料設定的設定金鑰。

說明	類型	預設值	詳細資訊

JSON 金鑰	類型	說明	屬性
設定 Allow-Listed 應用程式 JSON 金鑰： <code>com.microsoft.launcher.HomeScreen.Applications</code>	BundleArray	請參閱： 設定允許列出的應用程式	可讓您從裝置上安裝的應用程式中，定義一組可在主畫面上顯示的應用程式。您可以輸入想要顯示之應用程式的應用程式套件名稱來定義應用程式，例如， <code>com.android.settings</code> 讓設定可在主畫面上存取。您在本節中允許列出的應用程式應該已安裝在裝置上，才能顯示在主畫面上。 屬性： ■：應用程式套件名稱 ■：特定應用程式頁面特有的應用程式活動。如果此值是空的，則會使用預設應用程式頁面。
主畫面應用程式訂單 JSON 金鑰： <code>com.microsoft.launcher.HomeScreen.AppOrder</code>	BundleArray	請參閱： 主畫面應用程式訂單	可讓您在主畫面上指定應用程式訂單。 屬性： ■：如果您想要指定應用程式的位置，唯一支援的類型是 <code>application</code>。如果您想要指定 Web 連結的位置，則類型為 <code>weblink</code>。 ■：這會指定主畫面上的應用程式圖示位置。這會從左上方的位置 1 開始，然後由左至右、由上至下。 ■：這是用來指定應用程式順序的應用程式套件名稱。 ■：是特定應用程式頁面特有的應用程式活動。如果此值是空的，則會使用預設的應用程式頁面。此屬性用於應用程式。 ■：是特定應用程式頁面特有的應用程式活動。如果此值是空的，則會使用預設的應用程式頁面。此屬性用於應用程式。 ■：使用者按一下 Web 連結圖示之後要啟動的 URL。此屬性用於 Web 連結。
設定釘選的 Web 連結 JSON 金鑰： <code>com.microsoft.launcher.HomeScreen.WebLinks</code>	BundleArray	不適用	此金鑰可讓您將網站釘選到主畫面作為快速啟動圖示。如此一來，您就可以確定終端使用者可以快速且輕鬆地存取基本網站。您可以修改 [主畫面應用程式順序] 設定中每個 Web 連結圖示的位置。 屬性： ■：MS Launcher 主畫面上顯示的網頁連結標題。 ■：使用者按一下 Web 連結圖示之後要啟動的 URL。

'''	'''	'''	''
設定資料夾圖示圖形、開啟格式和捲動方向 JSON 金鑰: <code>com.microsoft.launcher.Folder.Style</code>	BundleArray	不適用	可讓您定義資料夾圖示的外觀，以及在 Microsoft Launcher 主畫面和擴充座上開啟資料夾的方式。 屬性： • folderShape: 此索引鍵可以設定為五個值之一：<code>Rounded_square</code>、<code>Square</code>、<code>Squircle</code>、<code>Round</code> 和 <code>Teardrop</code>。 • openFullScreen: 此索引鍵可以設定為下列其中一個值：<code>True</code> 或 <code>False</code>。如果設定為 <code>True</code>，則會在全螢幕中開啟資料夾。如果設定為 <code>False</code>，則不會在全螢幕中開啟資料夾。 • folderScroll: 此索引鍵可以設定為下列其中一個值：<code>vertical</code> 或 <code>horizontal</code>。預設值會設定為 <code>vertical</code>。
設定允許的資料夾圖示圖形、開啟格式和捲動方向使用者變更 JSON 金鑰: <code>com.microsoft.launcher.Folder.Style.UserChangeAllowed</code>	布林值	True	可讓您指定使用者是否可以變更 [資料夾樣式] 設定。 • 如果設定為 <code>True</code>，則只會針對初始部署強制執行資料夾的形狀、資料夾開啟的方式，以及資料夾捲動原則中所定義的方式。之後，將不會強制執行原則，以遵守使用者稍後可能所做的任何變更。 • 如果設定為 <code>False</code>，則為資料夾的形狀、資料夾開啟的方式，以及每次同步處理時會強制執行資料夾捲動的方式。

設定允許列出的應用程式

```
{
  "key": "com.microsoft.launcher.HomeScreen.Applications",
  "valueBundleArray":
  [
    {
      "managedProperty": [
        {
          "key": "package",
          "valueString": "com.android.settings"
        },
        {
          "key": "class",
          "valueString": ""
        }
      ]
    }
  ]
}
```

主畫面應用程式訂單


```
{
  "key": "com.microsoft.launcher.HomeScreen.AppOrder",
  "valueBundleArray": [
    {
      "managedProperty": [
        {
          "key": "type",
          "valueString": "application"
        },
        {
          "key": "position",
          "valueInteger": 1
        },
        {
          "key": "package",
          "valueString": "com.android.settings"
        },
        {
          "key": "class",
          "valueString": ""
        }
      ]
    }
  ]
}
```

設定釘選的 Web 連結

```
{
  "key": "com.microsoft.launcher.HomeScreen.WebLinks",
  "valueBundleArray": [
    {
      "managedProperty": [
        {
          "key": "label",
          "valueString": "weblink"
        },
        {
          "key": "link",
          "valueString": "https://www.microsoft.com"
        }
      ]
    }
  ]
},
{
  "key": "com.microsoft.launcher.HomeScreen.AppOrder",
  "valueBundleArray": [
    {
      "managedProperty": [
        {
          "key": "type",
          "valueString": "weblink"
        },
        {
          "key": "position",
          "valueInteger": 2
        },
        {
          "key": "label",
          "valueString": "Microsoft"
        },
        {
          "key": "link",
          "valueString": "https://www.microsoft.com"
        }
      ]
    }
  ]
}
]
```

Microsoft Launcher 組態範例

以下是包含所有可用組態金鑰的範例 JSON 腳本：

```
{
  "kind": "androidenterprise#managedConfiguration",
  "productId": "app:com.microsoft.launcher",
  "managedProperty": [
    {
      "key": "management_mode_key",
      "valueString": "Default"
    }
  ]
}
```

```

},
{
  "key": "com.microsoft.launcher.Feed.Enable.UserChangeAllowed",
  "valueBool": false
},
{
  "key": "com.microsoft.launcher.Feed.Enable",
  "valueBool": true
},
{
  "key": "com.microsoft.launcher.Wallpaper.Url.UserChangeAllowed",
  "valueBool": false
},
{
  "key": "com.microsoft.launcher.Wallpaper.Url",
  "valueString": "http://www.contoso.com/wallpaper.png"
},
{
  "key": "com.microsoft.launcher.HomeScreen.GridSize",
  "valueString": "5;5"
},
{
  "key": "com.microsoft.launcher.HomeScreen.Applications",
  "valueBundleArray": [
    {
      "managedProperty": [
        {
          "key": "package",
          "valueString": "com.ups.mobile.android"
        },
        {
          "key": "class",
          "valueString": ""
        }
      ]
    },
    {
      "managedProperty": [
        {
          "key": "package",
          "valueString": "com.microsoft.teams"
        },
        {
          "key": "class",
          "valueString": ""
        }
      ]
    }
  ]
},
{
  "key": "com.microsoft.launcher.HomeScreen.WebLinks",
  "valueBundleArray": [
    {
      "managedProperty": [
        {
          "key": "label",
          "valueString": "News"
        },
        {
          "key": "link",
          "valueString": "https://www.contoso.com"
        }
      ]
    }
  ]
},
{
  "key": "com.microsoft.launcher.HomeScreen.AppOrder.UserChangeAllowed",
  "valueBool": false
},
{
  "key": "com.microsoft.launcher.HomeScreen.AppOrder",
  "valueBundleArray": [
    {
      "managedProperty": [

```

```

        {
            "key": "type",
            "valueString": "application"
        },
        {
            "key": "position",
            "valueInteger": 17
        },
        {
            "key": "package",
            "valueString": "com.ups.mobile.android"
        },
        {
            "key": "class",
            "valueString": ""
        }
    ]
},
{
    "managedProperty": [
        {
            "key": "type",
            "valueString": "application"
        },
        {
            "key": "position",
            "valueInteger": 18
        },
        {
            "key": "package",
            "valueString": "com.microsoft.teams"
        },
        {
            "key": "class",
            "valueString": ""
        }
    ]
},
{
    "managedProperty": [
        {
            "key": "type",
            "valueString": "application"
        },
        {
            "key": "position",
            "valueInteger": 19
        },
        {
            "key": "package",
            "valueString": "com.microsoft.bing"
        },
        {
            "key": "class",
            "valueString": ""
        }
    ]
},
{
    "managedProperty": [
        {
            "key": "type",
            "valueString": "weblink"
        },
        {
            "key": "position",
            "valueInteger": 20
        },
        {
            "key": "label",
            "valueString": "News"
        },
        {
            "key": "link",
            "valueString": "https://www.contoso.com"
        }
    ]
}
    ]
}
}

```

後續步驟

- 如需 Android Enterprise 完全受控裝置的詳細資訊, 請參閱[設定 Android Enterprise 完全管理裝置的Intune註冊](#)。

使用適用於 iOS 和 Android 的 Edge 搭配 Microsoft Intune 來管理 Web 存取

2022/9/27 •

iOS 和 Android 版 Edge 的設計目的是要讓使用者流覽網頁並支援多重身分識別。使用者可以新增工作帳戶和個人帳戶以進行流覽。這兩個身分識別之間有完整的區隔，就像其他 Microsoft 行動應用程式所提供的一樣。

本功能適用於：

- iOS/iPadOS 14.0 或更新版本
- 已註冊裝置的 Android 8.0 或更新版本，以及未註冊裝置的 Android 9.0 或更新版本

NOTE

iOS 和 Android 版 Edge 不會取用使用者在其裝置上為原生瀏覽器設定的設定，因為適用於 iOS 和 Android 的 Edge 無法存取這些設定。

當您訂閱Enterprise Mobility + Security套件時，可以使用 Microsoft 365 資料最豐富且最廣泛的保護功能，其中包括Microsoft Intune和Azure Active Directory Premium功能，例如條件式存取。您至少會想要部署條件式存取原則，只允許從行動裝置連線到 iOS 和 Android 版 Edge，以及可確保流覽體驗受到保護的Intune應用程式保護原則。

NOTE

在 iOS 裝置上) (釘選 Web 應用程式的新網頁剪輯，將會在 iOS 和 Android 版 Edge 中開啟，而不是在需要在受保護的瀏覽器中開啟時開啟Intune Managed Browser。對於較舊的 iOS 網頁剪輯，您必須重新設定這些網頁剪輯的目標，以確保它們在 iOS 和 Android 版 Edge 中開啟，而不是在 Managed Browser 中開啟。

套用條件式存取

組織可以使用 Azure AD 條件式存取原則，以確保使用者只能使用適用於 iOS 和 Android 的 Edge 來存取公司或學校內容。若要這樣做，您需要以所有潛在使用者為目標的條件式存取原則。這些原則會在 [條件式存取：需要核准的用戶端應用程式或應用程式保護原則](#) 中說明。

請遵循使用行動 [裝置要求核准的用戶端應用程式或應用程式保護原則](#) 中的步驟，這會允許適用於 iOS 和 Android 的 Edge，但會封鎖其他行動裝置網頁瀏覽器連線到 Microsoft 365 端點。

NOTE

此原則可確保行動使用者可以從 iOS 和 Android 版 Edge 記憶體取所有 Microsoft 365 端點。此原則也會防止使用者使用 InPrivate 存取 Microsoft 365 端點。

使用條件式存取，您也可以將透過[Azure AD 應用程式 Proxy](#)公開給外部使用者的內部部署網站設為目標。

NOTE

若要利用應用程式型條件式存取原則，必須在 iOS 裝置上安裝 Microsoft Authenticator 應用程式。針對 Android 裝置，需要Intune 公司入口網站應用程式。如需詳細資訊，請參閱使用[Intune的應用程式型條件式存取](#)。

建立Intune應用程式保護原則

應用程式保護原則 (APP) 定義允許哪些應用程式，以及它們可對組織資料採取的動作。APP 中可用的選項可讓組織根據其特定需求量身打造保護。對某些人而言，實作完整案例所需的原則設定可能不明顯。為了協助組織排定行動用戶端端點強化的優先順序，Microsoft 為其適用於 iOS 和 Android 行動應用程式管理的應用程式資料

保護架構引進了分類法。

APP 資料保護架構會組織成三個不同的組態層級，每個層級會根據上一個層級來建置：

- **企業基本資料保護** (層級 1) 確保應用程式受到 PIN 保護並加密，並執行選擇性抹除作業。針對 Android 裝置，此層級會驗證 Android 裝置證明。這是一種進入層級設定，可在信箱原則Exchange Online提供類似的資料保護控制，並將 IT 和使用者母體引進 APP。
- **企業增強的資料保護** (層級 2) 引進 APP 資料外泄防護機制和最低 OS 需求。這是適用於大部分存取公司或學校資料之行動使用者的設定。
- **企業高資料保護** (層級 3) 引進進階資料保護機制、增強的 PIN 設定，以及 APP Mobile Threat Defense。此設定適用於存取高風險資料的使用者。

若要查看每個設定層級的特定建議，以及必須保護的最低應用程式，請 [檢閱使用應用程式保護原則的資料保護架構](#)。

無論裝置是否已在統一端點管理 (UEM) 解決方案中註冊，都必須使用[如何建立和指派應用程式保護原則](#)中的步驟，為 iOS 和 Android 應用程式建立Intune應用程式保護原則。這些原則至少必須符合下列條件：

- 它們包含所有 Microsoft 365 行動應用程式，例如 Edge、Outlook、OneDrive、Office 或 Teams，因為這可確保使用者可以安全的方式存取及操作任何 Microsoft 應用程式內的工作或學校資料。
- 它們會指派給所有使用者。這可確保所有使用者都受到保護，無論他們使用適用於 iOS 或 Android 的 Edge。
- 判斷哪個架構層級符合您的需求。大部分的組織都應該實作 **企業增強型資料保護** (層級 2) 中定義的設定，因為這可啟用資料保護和存取需求控制。

如需可用設定的詳細資訊，請參閱 [Android 應用程式保護原則設定](#) 和 [iOS 應用程式保護原則設定](#)。

IMPORTANT

若要對未在 Intune 中註冊的 Android 裝置上套用Intune應用程式保護原則，使用者也必須安裝Intune 公司入口網站。

在受原則保護的瀏覽器中單一登入與 Azure AD 連線的 Web 應用程式

適用於 iOS 和 Android 的 Edge 可以利用單一登入 (SSO)，(SaaS 和內部部署) 連線到 Azure AD 的所有 Web 應用程式。SSO 可讓使用者透過適用於 iOS 和 Android 的 Edge 存取 Azure AD 連線的 Web 應用程式，而不需要重新輸入其認證。

SSO 要求您的裝置必須由 iOS 裝置的 Microsoft Authenticator 應用程式或 Android 上的Intune 公司入口網站註冊。當使用者有上述任一項時，系統會在使用者移至受原則保護瀏覽器中的 Azure AD 連線 Web 應用程式時，提示他們註冊其裝置 (只有當他們的裝置尚未註冊) 時，才正確。向Intune所管理的使用者帳戶註冊裝置之後，該帳戶已針對 Azure AD 連線的 Web 應用程式啟用 SSO。

NOTE

裝置註冊是使用 Azure AD 服務的簡單簽入。它不需要完整裝置註冊，也不會在裝置上為 IT 提供任何額外的許可權。

使用應用程式設定來管理流覽體驗

iOS 和 Android 版 Edge 支援允許統一端點管理的應用程式設定，例如 Microsoft 端點管理員，系統管理員可自訂應用程式的行為。

應用程式設定可以透過已註冊裝置上的行動裝置管理 (MDM) OS 通道，(iOS 的受控[應用程式組態](#)通道或 Android 企業版[Android](#)) 通道，或透過 Intune 應用程式保護原則 (APP) 通道傳遞。iOS 和 Android 版 Edge 支援下列組態案例：

- 只允許公司或學校帳戶
- 一般應用程式組態設定
- 資料保護設定

IMPORTANT

針對需要在 Android 上註冊裝置的組態案例，必須在 Android Enterprise 中註冊裝置，而 Android 版 Edge 必須透過受控 Google Play 商店部署。如需詳細資訊，請參閱[設定 Android Enterprise 個人擁有工作設定檔裝置的註冊](#)和[新增受控 Android Enterprise 裝置的應用程式設定原則](#)。

每個組態案例都會強調其特定需求。例如，設定案例是否需要裝置註冊，因此可與任何 UEM 提供者搭配使用，或需要Intune應用程式保護原則。

IMPORTANT

應用程式設定金鑰會區分大小寫。使用適當的大小寫以確保設定生效。

NOTE

使用 Microsoft 端點管理員，透過 MDM OS 通道傳遞的應用程式設定稱為受控 ■ 應用程式組態原則 (ACP) ;透過應用程式保護原則通道傳遞的應用程式設定稱為受控 ■■ 應用程式組態原則。

只允許公司或學校帳戶

遵守我們最大且高度管制客戶的資料安全性與合規性原則是 Microsoft 365 價值的重要要素。有些公司需要擷取其公司環境中的所有通訊資訊，以及確保裝置僅用於公司通訊。為了支援這些需求，已註冊裝置上的 iOS 和 Android 版 Edge 可以設定為只允許在應用程式內布建單一公司帳戶。

您可以在這裡深入瞭解如何設定組織允許的帳戶模式設定：

- [Android 設定](#)
- [iOS 設定](#)

此設定案例僅適用於已註冊的裝置。不過，支援任何 UEM 提供者。如果您不是使用 Microsoft 端點管理員，您必須參閱 UEM 檔，以瞭解如何部署這些設定金鑰。

一般應用程式組態案例

iOS 和 Android 版 Edge 可讓系統管理員自訂數個應用程式內設定的預設組態。目前只有當 iOS 和 Android 版 Edge 已將Intune應用程式保護原則套用至已登入應用程式的公司或學校帳戶，且原則設定僅透過受控應用程式組態原則傳遞時，才會提供此功能。

IMPORTANT

Android 版 Edge 不支援受控 Google Play 中可用的Chromium設定。

Edge 支援下列組態設定：

- 新增索引標籤頁面體驗
- 書籤體驗
- 應用程式行為體驗
- Kiosk 模式體驗

不論裝置註冊狀態為何，這些設定都可以部署到應用程式。

新增索引標籤頁面體驗

當您登入 iOS 和 Android 版 Edge 時，開啟新的索引標籤頁面會提供熟悉的生產力內容，以及在單一檢視中組織與貴組織產業相關之新聞摘要的新樞紐。[\[新增索引標籤頁面\]](#) 體驗提供貴組織首頁、熱門網站和產業新聞的連結。

適用於 iOS 和 Android 的 Edge 為組織提供數個選項來調整新的索引標籤頁面體驗。

組織標誌和品牌色彩

這些設定可讓您自訂適用於 iOS 和 Android 的 Edge 新索引標籤頁面，以顯示您組織的標誌和品牌色彩作為頁面背景。

若要上傳貴組織的標誌和色彩，請先完成下列步驟：

1. 在 [Microsoft 端點管理員](#) 中，流覽至 [租使用者系統管理 > 自訂]。在 [設定] 旁，按一下 [編輯]。
2. 若要設定品牌的標誌，請在 [顯示在標頭] 旁選擇 [僅限組織標誌]。建議使用透明背景標誌。
3. 若要設定品牌的背景色彩，請選取 **主題色彩**。iOS 和 Android 版 Edge 會在 [新增索引標籤頁面] 上套用較淺的色彩陰影，以確保頁面具有高可讀性。

接下來，使用下列機碼/值組，將組織的商標提取到適用於 iOS 和 Android 的 Edge：

機碼	值
com.microsoft.intune.mam.managedbrowser.NewTabPage.BrandLogo	true 顯示組織的品牌標誌 false (預設) 不會公開標誌
com.microsoft.intune.mam.managedbrowser.NewTabPage.BrandColor	true 顯示組織的品牌色彩 false (預設) 不會公開色彩

首頁快捷方式

此設定可讓您在 [新增索引標籤頁面] 中設定適用於 iOS 和 Android 的 Edge 首頁快捷方式。當使用者在 iOS 和 Android 版 Edge 中開啟新的索引標籤時，您設定的首頁快捷方式會顯示為搜尋列下的第一個圖示。使用者無法在其 Managed 內容中編輯或刪除此快捷方式。首頁快捷方式會顯示您組織的名稱來加以區別。

機碼	值
com.microsoft.intune.mam.managedbrowser.homepage	指定有效的 URL。不正確的 URL 會作為安全性措施封鎖。 例如： <code>https://www.bing.com</code>

多個頂端網站快捷方式

與設定首頁快捷方式類似，您可以在 iOS 和 Android 版 Edge 的新索引標籤頁面上設定多個熱門網站快捷方式。使用者無法在受控內容中編輯或刪除這些快捷方式。注意：您總共可以設定 8 個快捷方式，包括首頁快捷方式。如果您已設定首頁快捷方式，該快捷方式將會覆寫第一個設定的前幾個網站。

機碼	值
com.microsoft.intune.mam.managedbrowser.managedTopSites	指定一組值 URL。每個頂端網站快捷方式都包含標題和 URL。使用字元分隔標題和 URL。例如： <code>GitHub https://github.com/ LinkedIn https://www.linkedin.com</code>

產業新聞

您可以在適用於 iOS 和 Android 的 Edge 內設定新的索引標籤頁面體驗，以顯示與您組織相關的產業新聞。當您啟用這項功能時，適用於 iOS 和 Android 的 Edge 會使用組織的功能變數名稱，從網路匯總有關貴組織、組織產業和競爭對手的新聞，讓您的使用者可以從 iOS 和 Android 版 Edge 內的集中式新索引標籤頁面找到相關的外部新聞。產業新聞預設為關閉。

機碼	值
com.microsoft.intune.mam.managedbrowser.NewTabPage.IndustryNews	true 是表示 在新索引標籤頁面上顯示產業新聞 false (預設) 會從 [新增索引標籤] 頁面隱藏產業新聞

首頁，而不是新的索引標籤頁面體驗

iOS 和 Android 版 Edge 可讓組織停用 [新增索引標籤頁面] 體驗，並在使用者開啟新的索引標籤時改為啟動網站。雖然這是支援的案例，但 Microsoft 建議組織利用 [新增索引標籤頁面] 體驗來提供與使用者相關的動態內容。

II	I
com.microsoft.intune.mam.managedbrowser.NewTabPage.CustomURL	指定有效的 URL。如果未指定 URL, 應用程式會使用 [新增索引標籤頁面] 體驗。不正確的 URL 會作為安全性措施封鎖。 例如: <code>https://www.bing.com</code>

書籤體驗

適用於 iOS 和 Android 的 Edge 為組織提供數個管理書籤的選項。

Managed 書籤

為了方便存取, 您可以設定使用者在使用適用於 iOS 和 Android 的 Edge 時可使用的書籤。

- 書籤只會出現在公司或學校帳戶中, 不會公開給個人帳戶。
- 使用者無法刪除或修改書籤。
- 書籤會出現在清單頂端。使用者建立的任何書籤都會出現在這些書籤下方。
- 如果您已啟用應用程式 Proxy 重新導向, 您可以使用 web 應用程式的內部或外部 URL 來新增應用程式 Proxy Web 應用程式。
- 請確定您在將所有 URL 輸入清單時, 以 HTTP:// 或 HTTPS:// 為前置詞。
- 書籤會建立在以 Azure Active Directory 中定義的組織名稱命名的資料夾中。

II	I
com.microsoft.intune.mam.managedbrowser.bookmarks	此組態的值是書籤清單。每個書籤都包含書籤標題和書籤 URL。使用 字元分隔標題和 URL 。 例如: <code>Microsoft Bing https://www.bing.com</code> 若要設定多個書籤, 請使用雙字元 分隔每個配對。 例如: <pre>Microsoft Bing https://www.bing.com Contoso https://www.contoso.com</pre>

我的應用程式書籤

根據預設, 使用者會在 iOS 和 Android 版 Edge 內的組織資料夾內設定我的應用程式書籤。

II	I
com.microsoft.intune.mam.managedbrowser.MyApps	true (預設) 在 iOS 和 Android 版 Edge 書籤內顯示我的應用程式 false 會隱藏 iOS 和 Android 版 Edge 內的我的應用程式

應用程式行為體驗

適用於 iOS 和 Android 的 Edge 為組織提供數個管理應用程式行為的選項。

Azure AD 密碼單一登入

Azure ACTIVE Directory 提供的 Azure AD 密碼單一登入 (SSO) 功能, 可將使用者存取管理帶入不支援身分識別同盟的 Web 應用程式。根據預設, 適用於 iOS 和 Android 的 Edge 不會使用 Azure AD 認證執行 SSO。如需詳細資訊, 請 [參閱將密碼型單一登入新增至應用程式](#)。

II	I
com.microsoft.intune.mam.managedbrowser.PasswordSSO	■ 已啟用 Azure AD 密碼 SSO false (預設) Azure AD 密碼 SSO 已停用

預設通訊協定處理常式

根據預設, 當使用者未在 URL 中指定通訊協定時, 適用於 iOS 和 Android 的 Edge 會使用 HTTPS 通訊協定處理常式。一般而言, 這是最佳做法, 但可以停用。

II	I
com.microsoft.intune.mam.managedbrowser.defaultHTTPS	true (預設) 通訊協定處理常式為 HTTPS false 預設通訊協定處理常式為 HTTP

停用個人化的資料共用

根據預設，適用於 iOS 和 Android 的 Edge 會提示使用者使用資料收集和共用流覽歷程記錄，以個人化其流覽體驗。組織可以防止向使用者顯示此提示，以停用此資料共用。

名稱	值
com.microsoft.intune.mam.managedbrowser.disableShareUsageData	true 會停用此提示，使使用者無法顯示 false (預設) 提示使用者共用使用量資料
com.microsoft.intune.mam.managedbrowser.disableShareBrowsingHistory	true 會停用此提示，使使用者無法顯示 false (預設) 提示使用者共用流覽歷程記錄

停用特定功能

iOS 和 Android 版 Edge 可讓組織停用預設啟用的特定功能。若要停用這些功能，請設定下列設定：

名稱	值
com.microsoft.intune.mam.managedbrowser.disabledFeatures	password 會停用提供為終端使用者儲存密碼的提示 inprivate 停用 InPrivate 瀏覽 autofill 會停用「儲存和填滿位址」和「儲存並填入付款資訊」。即使先前儲存的資訊，也會停用自動填寫。 若要停用多個功能，請使用 <code> </code> 分隔值。例如， <code>inprivate password</code> 會停用 InPrivate 和密碼儲存體。

停用擴充功能

您可以在 iOS 和 Android 版 Edge 內停用擴充功能架構，例如 Coupons，以防止使用者安裝或使用任何預先設定的應用程式延伸模組。若要這樣做，請設定下列設定：

名稱	值
com.microsoft.intune.mam.managedbrowser.disableExtensionFramework	true 會停用延伸模組架構 false (預設) 啟用擴充架構

NOTE

iOS 版 Edge 不支援停用擴充功能。

控制 Cookie 模式

您可以控制網站是否可以在 Android 版 Edge 中儲存使用者的 Cookie。若要這樣做，請設定下列設定：

名稱	值
com.microsoft.intune.mam.managedbrowser.cookieControlsMode	0 (預設) 允許 Cookie 1 個區塊非 Microsoft Cookie 2 在 InPrivate 模式中封鎖非 Microsoft Cookie 3 封鎖所有 Cookie

NOTE

iOS 版 Edge 不支援控制 Cookie。

Android 裝置上的 Kiosk 模式體驗

您可以使用下列設定，將 Android 版 Edge 啟用為 kiosk 應用程式：

名稱	值
com.microsoft.intune.mam.managedbrowser.enableKioskMode	true 會啟用 Android 版 Edge 的 kiosk 模式 false (預設) 停用 kiosk 模式

II	I
com.microsoft.intune.mam.managedbrowser.showAddressBarInKioskMode	true 顯示 kiosk 模式的網址列 false (啟用 kiosk 模式時, 預設) 會隱藏網址列
com.microsoft.intune.mam.managedbrowser.showBottomBarInKioskMode	true 顯示 kiosk 模式的底部動作列 false (啟用 kiosk 模式時, 預設) 會隱藏底部列

資料保護應用程式組態案例

當應用程式由 Microsoft 端點管理員管理, 且Intune應用程式保護原則套用至已登入應用程式的公司或學校帳戶, 且原則設定僅透過受控應用程式應用程式組態原則傳遞時, iOS 和 Android 版 Edge 支援下列資料保護設定的應用程式設定原則:

- 管理帳戶同步處理
- 管理受限制的網站
- 管理 Proxy 設定
- 管理 NTLM 單一登入網站

不論裝置註冊狀態為何, 這些設定都可以部署到應用程式。

管理帳戶同步處理

根據預設, Microsoft Edge 同步可讓使用者在其所有已登入的裝置上存取其流覽資料。同步處理支援的資料包括:

- 我的最愛
- 密碼
- 自動填滿表單專案 (位址和更多)

同步處理功能是透過使用者同意來啟用, 而且使用者可以開啟或關閉上述每個資料類型的同步處理。如需詳細資訊, 請 [參閱 Microsoft Edge 同步處理](#)。

組織能夠在 iOS 和 Android 上停用 Edge 同步處理。

II	I
com.microsoft.intune.mam.managedbrowser.account.syncDisabled	true 會停用 Edge 同步處理 false (預設) 允許 Edge 同步處理

管理受限制的網站

組織可以定義使用者可以在 iOS 和 Android 版 Edge 的工作或學校帳戶內容中存取哪些網站。如果您使用允許清單, 您的使用者就只能存取明確列出的網站。如果您使用封鎖清單, 使用者可以存取所有網站, 但明確封鎖的網站除外。您應該只強制使用允許或封鎖的清單, 而不是兩者。如果您同時強制使用這兩者, 則只接受允許的清單。

組織也會定義當使用者嘗試流覽至受限制的網站時會發生什麼情況。根據預設, 允許轉換。如果組織允許, 則可在個人帳戶內容、Azure AD 帳戶的 InPrivate 內容中開啟受限制的網站, 或是否完全封鎖網站。如需支援之各種案例的詳細資訊, 請參閱 [Microsoft Edge 行動裝置版中受限制的網站轉換](#)。藉由允許轉換體驗, 組織的使用者會保持受到保護, 同時保護公司資源的安全。

NOTE

iOS 和 Android 版 Edge 只有在直接存取網站時, 才能封鎖網站的存取。當使用者使用中繼服務 (例如翻譯服務) 存取網站時, 它不會封鎖存取。

使用下列機碼/值組, 為 iOS 和 Android 版 Edge 設定允許或封鎖的網站清單。

名稱	說明
com.microsoft.intune.mam.managedbrowser.AllowListURLs	索引鍵的對應值是 URL 清單。您可以輸入您想要允許的所有 URL 做為單一值，並以管道 字元分隔。 ■： URL1 URL2 URL3 http://www.contoso.com/ https://www.bing.com/ https://expenses.conto
com.microsoft.intune.mam.managedbrowser.BlockListURLs	索引鍵的對應值是 URL 清單。您輸入您要封鎖的所有 URL 做為單一值，並以管道 字元分隔。 ■： URL1 URL2 URL3 http://www.contoso.com/ https://www.bing.com/ https://expenses.conto
com.microsoft.intune.mam.managedbrowser.AllowTransitionOnBlock	true (預設) 允許適用於 iOS 和 Android 的 Edge 轉換受限制的網站。當個人帳戶未停用時，系統會提示使用者切換至個人內容以開啟受限制的網站，或新增個人帳戶。如果 com.microsoft.intune.mam.managedbrowser.openInPrivateIfBlocked 設定為 true，則使用者能夠在 InPrivate 內容中開啟受限制的網站。 false 會防止適用於 iOS 和 Android 的 Edge 轉換使用者。使用者只會看到一則訊息，指出他們嘗試存取的網站遭到封鎖。
com.microsoft.intune.mam.managedbrowser.openInPrivateIfBlocked	true 允許在 Azure AD 帳戶的 InPrivate 內容中開啟受限制的網站。如果 Azure AD 帳戶是針對 iOS 和 Android 在 Edge 中設定的唯一帳戶，則會在 InPrivate 內容中自動開啟受限制的網站。如果使用者已設定個人帳戶，系統會提示使用者選擇開啟 InPrivate 或切換至個人帳戶。 false (預設) 需要在使用者的個人帳戶中開啟受限制的網站。如果停用個人帳戶，則會封鎖網站。 若要讓此設定生效，com.microsoft.intune.mam.managedbrowser.AllowTransitionOnBlock 必須設定為 true。
com.microsoft.intune.mam.managedbrowser.durationOfOpenInPrivateSnackBar	輸入使用者會看到餐點列通知的秒數：「您的組織已封鎖存取此網站。我們已在 InPrivate 模式中開啟它，讓您存取網站。」根據預設，即會顯示 7 秒的餐點通知。

不論定義的允許清單或封鎖清單設定為何，一律允許下列網站：

- https://*.microsoft.com/*
- http://*.microsoft.com/*
- https://microsoft.com/*
- http://microsoft.com/*
- https://*.windowsazure.com/*
- https://*.microsoftonline.com/*
- https://*.microsoftonline-p.com/*

允許和封鎖網站清單的 URL 格式

您可以使用各種 URL 格式來建置允許/封鎖的網站清單。下表詳細說明這些允許的模式。

- 請確定您在將所有 URL 輸入清單時，以 HTTP:// 或 HTTPS:// 為前置詞。
- 您可以根據下列允許模式清單中的規則，使用萬用字元符號 (*)。
- 萬用字元只能比對部分 (例如， news-contoso.com) 或主機名稱的整個元件 (例如， host.contoso.com) 或路徑的整個部分，以正斜線分隔 (www.contoso.com/images)。
- 您可以在位址中指定埠號碼。如果您未指定埠號碼，則使用的值為：
 - 埠 80 for HTTP
 - 埠 443 for HTTPS

- 不支援針對埠號碼使用萬用字元。例如，`http://www.contoso.com:*` 和 `http://www.contoso.com:*/` 不受支援。

URL	說明	包含	排除
<code>http://www.contoso.com</code>	比對單一頁面	<code>www.contoso.com</code>	<code>host.contoso.com</code> <code>www.contoso.com/images</code> <code>contoso.com/</code>
<code>http://contoso.com</code>	比對單一頁面	<code>contoso.com/</code>	<code>host.contoso.com</code> <code>www.contoso.com/images</code> <code>www.contoso.com</code>
<code>http://www.contoso.com/*</code>	比對開頭為 <code>www</code> 的所有 URL	<code>www.contoso.com</code> <code>www.contoso.com/images</code> <code>www.contoso.com/videos/tvshows</code>	<code>host.contoso.com</code> <code>host.contoso.com/images</code>
<code>http://*.contoso.com/*</code>	比對 下方 的所有子域	<code>developer.contoso.com/resources</code> <code>news.contoso.com/images</code> <code>news.contoso.com/videos</code>	<code>contoso.host.com</code> <code>news-contoso.com</code>
<code>http://*contoso.com/*</code>	比對以 <code>contoso.com</code> 結尾的所有子域	<code>news-contoso.com</code> <code>news-contoso.com.com/daily</code>	<code>news-contoso.host.com</code> <code>news.contoso.com</code>
<code>http://www.contoso.com/images</code>	比對單一資料夾	<code>www.contoso.com/images</code>	<code>www.contoso.com/images/dogs</code>
<code>http://www.contoso.com:80</code>	使用埠號碼比對單一頁面	<code>www.contoso.com:80</code>	
<code>https://www.contoso.com</code>	比對單一且安全的頁面	<code>www.contoso.com</code>	<code>www.contoso.com</code>
<code>http://www.contoso.com/images/*</code>	比對單一資料夾和所有子資料夾	<code>www.contoso.com/images/dogs</code> <code>www.contoso.com/images/cats</code>	<code>www.contoso.com/videos</code>

- 以下是您無法指定的一些輸入範例：

- `*.com`
- `*.contoso/*`
- `www.contoso.com/*images`
- `www.contoso.com/*images*pigs`
- `www.contoso.com/page*`
- IP 位址
- `https://*`
- `http://*`
- `http://www.contoso.com:*`
- `http://www.contoso.com: /*`

管理 Proxy 設定

您可以一起使用適用於 iOS 和 Android 的 Edge 和 [Azure AD 應用程式 Proxy](#)，讓使用者能夠存取其行動裝置上的內部網路網站。例如：

- 使用者正在使用 Outlook 行動裝置應用程式，該應用程式受到Intune保護。然後他們會在電子郵件中按一下內部網路網站的連結，而適用於 iOS 和 Android 的 Edge 會辨識此內部網路網站已透過應用程式 Proxy向使用者公開。使用者會透過應用程式 Proxy自動路由傳送，以使用任何適用的多重要素驗證和條件式存取進行驗證，然後再連線到內部網路網站。使用者現在可以存取內部網站，即使是在其行動裝置上，Outlook 中的連結也能如預期般運作。
- 使用者在其 iOS 或 Android 裝置上開啟適用於 iOS 和 Android 的 Edge。如果適用於 iOS 和 Android 的 Edge 受到Intune保護，且已啟用應用程式 Proxy，則使用者可以使用其使用的內部 URL 移至內部網路網站。iOS 和

Android 版 Edge 可辨識此內部網路網站已透過應用程式 Proxy 向使用者公開。使用者會自動透過應用程式 Proxy 路由傳送，以在到達內部網路網站之前進行驗證。

前置作業：

- 透過 Azure AD 應用程式 Proxy 來設定內部應用程式。
 - 若要設定應用程式 Proxy 和發佈應用程式，請參閱 [安裝檔](#)。
 - 確定已將使用者指派給 Azure AD 應用程式 Proxy 應用程式，即使應用程式已設定為傳遞預先驗證類型也一般。
- 適用於 iOS 和 Android 的 Edge 應用程式必須已指派 [Intune 應用程式保護原則](#)。
- Microsoft 應用程式的應用程式保護原則必須將 [限制 Web 內容傳輸與其他應用程式 的資料傳輸] 設定設為 Microsoft Edge。

NOTE

iOS 和 Android 版 Edge 會根據上次成功的重新整理事件，更新應用程式 Proxy 重新導向資料。每當最後一個成功的重新整理事件大於一小時時，就會嘗試更新。

具有下列索引鍵/值組的 iOS 目標 Edge，以啟用應用程式 Proxy：

II	I
com.microsoft.intune.mam.managedbrowser.AppProxyRedirection	true 會啟用 Azure AD 應用程式 Proxy 重新導向案例 false (預設) 防止 Azure AD 應用程式 Proxy 案例

NOTE

Android 版 Edge 不會取用此金鑰。相反地，只要已登入的 Azure AD 帳戶已套用應用程式保護原則，Android 版 Edge 就會自動取用 Azure AD 應用程式 Proxy 設定。

如需如何搭配使用適用於 iOS 和 Android 的 Edge 和 Azure AD 應用程式 Proxy，以順暢 (和受保護) 存取內部部署 Web 應用程式的詳細資訊，請參閱 [更好的一起：Intune 和 Azure Active Directory 小組合作以改善使用者存取](#)。此部落格文章參考 Intune Managed Browser，但內容也適用於 iOS 和 Android 版 Edge。

管理 NTLM 單一登入網站

組織可能需要使用者向 NTLM 進行驗證，才能存取內部網路網站。根據預設，系統會提示使用者在每次存取需要 NTLM 驗證的網站時輸入認證，因為 NTLM 認證快取已停用。

組織可以為特定網站啟用 NTLM 認證快取。針對這些網站，在使用者輸入認證並成功驗證之後，預設會快取認證 30 天。

II	I
com.microsoft.intune.mam.managedbrowser.NTLMSSOURLs	索引鍵的對應值是 URL 清單。您可以輸入您想要允許的所有 URL 做為單一值，並以管道 字元分隔。 ■： URL1 URL2 http://app.contoso.com/ https://expenses.contoso.com 如需支援之 URL 格式類型的詳細資訊，請參閱 允許和封鎖網站清單的 URL 格式 。
com.microsoft.intune.mam.managedbrowser.durationOfNTLMSSO	快取認證的時數，預設值為 720 小時

使用 Microsoft 端點管理員 部署應用程式組態案例

如果您使用 Microsoft 端點管理員 作為行動應用程式管理提供者，下列步驟可讓您建立受控應用程式應用程式設定原則。建立組態之後，您可以將其設定指派給使用者群組。

1. 登入[Microsoft 端點管理員](#)。
2. 選取 [應用程式]，然後選取 [應用程式設定原則]。
3. 在 [應用程式組態 原則] 刀鋒視窗中，選擇 [新增]，然後選取 [管理的應用程式]。
4. 在 [基本概念] 區段上，輸入應用程式組態設定的 [名稱] 和選擇性 [描述]。
5. 針對 [公用應用程式]，選擇 [選取公用應用程式]，然後在 [目標應用程式] 刀鋒視窗上選取 iOS 和 Android 版 Edge，方法是選取 iOS 和 Android 平臺應用程式。按一下 [選取] 以儲存選取的公用應用程式。
6. 按 [下一步] 以完成應用程式設定原則的基本設定。
7. 在 [設定] 區段上，展開 [Edge 組態設定]。
8. 如果您想要管理資料保護設定，請據以設定所需的設定：

- 針對 應用程式 Proxy 重新導向，請從可用的選項中選擇：啟用、停用 (預設)。
- 針對 [首頁快捷方式 URL]，指定包含 前置詞 的有效 URL HTTP:// 或 HTTPS://。不正確的 URL 會作為安全性措施封鎖。
- 針對 [受管理的書籤]，指定標題和有效的 URL，其中包含 HTTP:// 或 HTTPS:// 的前置詞。
- 針對 [允許的 URL]，指定有效的 URL (只允許這些 URL;無法存取其他網站)。如需支援之 URL 格式類型的詳細資訊，請參閱 [允許和封鎖網站清單的 URL 格式](#)。
- 針對 [封鎖的 URL]，指定有效的 URL (只有這些 URL 會被封鎖)。如需支援之 URL 格式類型的詳細資訊，請參閱 [允許和封鎖網站清單的 URL 格式](#)。
- 針對 [將受限制的網站重新導向至個人內容]，請從可用的選項中選擇：[啟用 (預設)]、[停用]。

NOTE

當原則中同時定義允許的 URL 和封鎖的 URL 時，只會接受允許的清單。

9. 如果您想要在上述原則中未公開其他應用程式組態設定，請展開 [一般組態設定] 節點，並據以輸入機碼值組。
10. 當您完成設定時，請選擇 [下一步]。
11. 在 [指派] 區段上，選擇 [選取要包含的群組]。選取您要指派應用程式設定原則的 Azure AD 群組，然後選擇 [選取]。
12. 當您完成指派時，請選擇 [下一步]。
13. 在 [建立應用程式設定原則檢閱 + 建立] 刀鋒視窗上，檢閱已設定的設定，然後選擇 [建立]。

新建立的設定原則會顯示在 [應用程式 設定] 刀鋒視窗上。

使用適用於 iOS 和 Android 的 Edge 來存取受控應用程式記錄

已在其 iOS 或 Android 裝置上安裝適用於 iOS 和 Android 版 Edge 的使用者，可以檢視所有 Microsoft 已發佈應用程式的管理狀態。他們可以使用下列步驟傳送記錄，以針對受控 iOS 或 Android 應用程式進行疑難排解：

1. 在您的裝置上開啟適用於 iOS 和 Android 的 Edge。
2. 在 [位址] 方塊中輸入 `about:intunehelp`。
3. 適用於 iOS 和 Android 的 Edge 會啟動疑難排解模式。

如需儲存在應用程式記錄中的設定清單，請參閱 [檢閱用戶端應用程式保護記錄](#)。

若要瞭解如何檢視 Android 裝置上的記錄，請參閱 [透過電子郵件將記錄傳送給 IT 系統管理員](#)。

在 Chromium 與 iOS 之間切換網路堆疊

網路架構的層稱為網路堆疊。網路堆疊的層級廣泛分成多個區段，例如網路介面、網路驅動程式介面規格 (NDIS)、通訊協定堆疊、系統驅動程式和User-Mode應用程式。

根據預設，iOS 和 Android 版 Edge 都會使用Chromium網路堆疊進行內部網路通訊，包括 VPN。iOS 版 Edge 也提供用於網路通訊的 iOS 網路堆疊。

組織可以藉由設定下列設定來修改其網路堆疊喜好設定。

¶	¶
com.microsoft.intune.mam.managedbrowser.NetworkStackPref	0 (預設) 使用Chromium網路堆疊 1 使用 iOS 網路堆疊

NOTE
建議Chromium網路堆疊。當您遇到網路問題時，請使用 iOS 網路堆疊，例如特別是 VPN。

後續步驟

- 什麼是應用程式保護原則？
- Microsoft Intune 的應用程式組態原則

使用 Microsoft Intune 管理適用於 iOS 和 Android 的 Office 共同作業體驗

2022/9/27 •

適用於 iOS 和 Android 的 Office 提供數個主要優點，包括：

- 結合 Word、Excel 和 PowerPoint 的方式可簡化下載或切換應用程式較少的體驗。相較於安裝個別應用程式，其需要的手機儲存體要少得多，同時維持現有行動裝置應用程式已知道和使用的所有功能。
- 整合 Office Lens 技術，以將影像轉換成可編輯的 Word 和 Excel 檔、掃描 PDF，以及擷取具有自動數位增強功能的白板等功能，讓內容更容易閱讀。
- 為在手機上工作時經常遇到的常見工作新增功能，例如製作快速筆記、簽署 PDF、掃描 QR 代碼，以及在裝置之間傳輸檔案。

當您訂閱Enterprise Mobility + Security套件時，可以使用 Microsoft 365 資料最豐富且最廣泛的保護功能，其中包括Microsoft Intune和Azure Active Directory Premium功能，例如條件式存取。您至少會想要部署條件式存取原則，以允許從行動裝置連線到 iOS 和 Android 版 Office，以及可確保共同作業體驗受到保護的Intune應用程式保護原則。

套用條件式存取

組織可以使用 Azure AD 條件式存取原則，確保使用者只能使用 Office for iOS 和 Android 存取公司或學校內容。若要這樣做，您需要以所有潛在使用者為目標的條件式存取原則。這些原則會在 [條件式存取：需要核准的用戶端應用程式或應用程式保護原則](#) 中說明。

1. 請遵循使用行動 [裝置要求核准的用戶端應用程式或應用程式保護原則](#) 中的步驟，這會允許適用於 iOS 和 Android 的 Office，但會封鎖協力廠商支援 OAuth 的行動裝置用戶端連線到 Microsoft 365 端點。

NOTE

此原則可確保行動使用者可以使用適用的應用程式存取所有 Microsoft 365 端點。

NOTE

若要利用應用程式型條件式存取原則，必須在 iOS 裝置上安裝 Microsoft Authenticator 應用程式。針對 Android 裝置，需要Intune 公司入口網站應用程式。如需詳細資訊，請參閱使用[Intune的應用程式型條件式存取](#)。

建立Intune應用程式保護原則

應用程式保護原則 (APP) 定義允許哪些應用程式，以及它們可對組織資料採取的動作。APP 中可用的選項可讓組織根據其特定需求量身打造保護。對某些人而言，實作完整案例所需的原則設定可能不明顯。為了協助組織排定行動用戶端端點強化的優先順序，Microsoft 為其適用於 iOS 和 Android 行動應用程式管理的應用程式資料保護架構引進了分類法。

APP 資料保護架構會組織成三個不同的組態層級，每個層級會根據上一個層級來建置：

- **企業基本資料保護** (層級 1) 確保應用程式受到 PIN 保護並加密，並執行選擇性抹除作業。針對 Android 裝置，此層級會驗證 Android 裝置證明。這是一種進入層級設定，可在信箱原則Exchange Online提供類似的資料保護控制，並將 IT 和使用者母體引進 APP。
- **企業增強的資料保護** (層級 2) 引進 APP 資料外泄防護機制和最低 OS 需求。這是適用於大部分存取公司或

學校資料之行動使用者的設定。

- **企業高資料保護** (層級 3) 引進進階資料保護機制、增強的 PIN 設定，以及 APP Mobile Threat Defense。此設定適用於存取高風險資料的使用者。

若要查看每個設定層級的特定建議，以及必須保護的最低應用程式，請 [檢閱使用應用程式保護原則的資料保護架構](#)。

無論裝置是否已在統一端點管理 (UEM) 解決方案中註冊，都必須使用[如何建立和指派應用程式保護原則](#)中的步驟，為 iOS 和 Android 應用程式建立Intune應用程式保護原則。這些原則至少必須符合下列條件：

1. 它們包含所有 Microsoft 365 行動應用程式，例如 Edge、Outlook、OneDrive、Office 或 Teams，因為這可確保使用者可以安全的方式存取及操作任何 Microsoft 應用程式內的工作或學校資料。
2. 它們會指派給所有使用者。這可確保所有使用者都受到保護，無論他們使用 Office for iOS 或 Android。
3. 判斷哪個架構層級符合您的需求。大部分的組織都應該實作 **企業增強型資料保護** (層級 2) 中定義的設定，因為這可啟用資料保護和存取需求控制。

如需可用設定的詳細資訊，請參閱 [Android 應用程式保護原則設定](#) 和 [iOS 應用程式保護原則設定](#)。

IMPORTANT

若要對未在 Intune 中註冊的 Android 裝置上套用Intune應用程式保護原則，使用者也必須安裝Intune 公司入口網站。

利用應用程式設定

iOS 版和 Android 版 Office 支援允許統一端點管理的應用程式設定，例如 Microsoft 端點管理員，系統管理員可自訂應用程式的行為。

應用程式設定可以透過已註冊裝置上的行動裝置管理 (MDM) OS 通道，(iOS 的受控[應用程式組態](#)通道或 Android 企業版[Android](#)) 通道，或透過 Intune 應用程式保護原則 (APP) 通道傳遞。適用於 iOS 和 Android 的 Office 支援下列設定案例：

- 只允許公司或學校帳戶
- 一般應用程式設定
- 資料保護設定

IMPORTANT

針對需要在 Android 上註冊裝置的設定案例，裝置必須在 Android Enterprise 中註冊，Android 版 Office必須透過受控 Google Play 商店部署。如需詳細資訊，請參閱[設定 Android Enterprise 個人擁有工作設定檔裝置的註冊](#) 和 [新增受控 Android Enterprise 裝置的應用程式設定原則](#)。

每個組態案例都會強調其特定需求。例如，設定案例是否需要裝置註冊，因此可與任何 UEM 提供者搭配使用，或需要Intune應用程式保護原則。

IMPORTANT

應用程式設定金鑰會區分大小寫。使用適當的大小寫以確保設定生效。

NOTE

使用 Microsoft 端點管理員，透過 MDM OS 通道傳遞的應用程式設定稱為受控  應用程式組態原則 (ACP) ;透過應用程式保護原則通道傳遞的應用程式設定稱為受控  應用程式組態原則。

只允許公司或學校帳戶

遵守我們最大且高度管制客戶的資料安全性與合規性原則是 Microsoft 365 價值的重要要素。有些公司需要擷取其公司環境中的所有通訊資訊，以及確保裝置僅用於公司通訊。若要支援這些需求，可將已註冊裝置上的 Android 版 Office 設定為只允許在應用程式內布建單一公司帳戶。

您可以在這裡深入瞭解如何設定組織允許的帳戶模式設定：

- [Android 設定](#)
- [iOS 設定](#)

此設定案例僅適用於已註冊的裝置。不過，支援任何 UEM 提供者。如果您不是使用 Microsoft 端點管理員，您必須參閱 UEM 檔，以瞭解如何部署這些設定金鑰。

一般應用程式組態案例

iOS/iPadOS 和 Android 版 Office 可讓系統管理員使用 [iOS/iPadOS](#) 或 [Android](#) 應用程式設定原則來自訂數個應用程式內設定的預設組態。這項功能會透過任何 UEM 提供者提供給已註冊的裝置，以及在 Office for iOS 和 Android 套用 Intune 應用程式保護原則時未註冊的裝置。

NOTE

如果應用程式保護原則以使用者為目標，建議您在受控  註冊模型中部署一般應用程式組態設定。這可確保應用程式組態原則同時部署到已註冊的裝置和未註冊的裝置。

Office 支援下列組態設定：

- 管理建立自黏便箋
- 設定增益集喜好設定
- 在預覽版中管理在 Android 版 Office 應用程式上執行的 Teams 應用程式 ()

管理建立自黏便箋

根據預設，適用於 iOS 和 Android 的 Office 可讓使用者建立自黏便箋。對於具有 Exchange Online 信箱的使用者，記事會同步處理到使用者的信箱。對於具有內部部署信箱的使用者，這些附注只會儲存在本機裝置上。

「	「
com.microsoft.office.NotesCreationEnabled	true (預設) 可為公司或學校帳戶建立自黏便箋 false 會停用自黏便箋建立公司或學校帳戶

設定增益集喜好設定

針對執行 Office 的 iOS/iPadOS 裝置，您 (系統管理員) 可以設定是否啟用 Office 增益集。您可以使用 Intune 中的 [應用程式設定原則](#) 來部署這些應用程式設定。

「	「
com.microsoft.office.OfficeWebAddinDisableAllCatalogs	true (預設) 停用整個增益集平臺 false 會啟用增益集平臺

如果您需要為 iOS 裝置啟用或停用平臺的 Office 市集部分，您可以使用下列金鑰。

「	「

「	「
com.microsoft.office.OfficeWebAddinDisableOMEXCatalog	true (預設) 只停用平臺的 Office 市集部分 false 會啟用平臺的 Office 市集部分 ■ : 側載會繼續運作。

如需新增設定金鑰的詳細資訊，請 [參閱為受控 iOS/iPadOS 裝置新增應用程式設定原則](#)。

在預覽版中管理在 Android 版 Office 應用程式上執行的 Teams 應用程式 0

Teams 個人索引標籤應用程式已在目標發行版本中預覽 Office.com 和 Outlook 桌上出版，IT 系統管理員可以使用 Teams 系統管理中心建立 [自訂許可權](#) 原則，並將 [這些原則指派給使用者](#)，以管理 Teams 應用程式的存取權。您現在也可以在適用於 Android 的 Office 應用程式中，在預覽版中執行 Teams 個人索引標籤應用程式。使用 [Microsoft Teams JavaScript 用戶端 SDK v2](#) (2.0.0 版) 和 [Teams 應用程式資訊清單](#) (1.13 版建置的 Teams 個人索引標籤應用程式) 會出現在 Android 版 Office 應用程式的 [應用程式] 功能表底下。

Android 版 Office 應用程式可能有其他特定的管理需求。您可能想要：

- 只允許組織中的特定使用者在適用於 Android 的 Office 應用程式上嘗試增強的 Teams 應用程式，或
- 禁止組織中的所有使用者在適用於 Android 的 Office 應用程式上使用增強的 Teams 應用程式。

若要管理這些專案，您可以使用下列金鑰：

「	「
com.microsoft.office.officemobile.TeamsApps.IsAllowed	true (預設) 啟用 Android 版 Office 應用程式上的 Teams 應用程式 false 會停用 Android 版 Office 應用程式上的 Teams 應用程式

受控裝置和受控應用程式都可以使用此金鑰。

資料保護應用程式組態案例

當應用程式由 Microsoft 端點管理員管理時，Office for iOS 和 Android 支援下列資料保護設定的應用程式組態原則，且 Intune 應用程式保護原則會套用至已登入應用程式的公司或學校帳戶，且原則設定只會透過受控應用程式應用程式組態原則傳遞：

- 透過 [傳輸檔案] 動作管理檔案傳輸
- 透過共用鄰近動作管理檔案傳輸

不論裝置註冊狀態為何，這些設定都可以部署到應用程式。

管理檔案傳輸

根據預設，適用於 iOS 和 Android 的 Office 可讓使用者使用各種機制來共用內容：

- 如果檔案裝載于 OneDrive 或 SharePoint 中，使用者可以直接在檔案內起始共用要求。
- 使用者可以使用 [傳輸 檔案] 動作，將檔案傳輸至桌面系統。
- 使用者可以使用 [共用 鄰近] 動作，將檔案共用到附近的行動裝置。

[傳輸檔案] 和 [共用鄰近] 動作僅適用於未受應用程式保護原則保護的媒體、本機檔案和檔案。

「	「
com.microsoft.office.ShareNearby.IsAllowed.IntuneMAMOnly	true (預設) 啟用公司或學校帳戶的共用鄰近功能 false 會停用公司或學校帳戶的共用鄰近功能

[[	]
com.microsoft.office.TransferFiles.IsAllowed.IntuneMAMOnly	true (預設) 啟用公司或學校帳戶的傳輸檔案功能 false 會停用公司或學校帳戶的傳輸檔案功能

使用 Microsoft 端點管理員 部署應用程式組態案例

如果您使用 Microsoft 端點管理員 作為行動應用程式管理提供者，請參閱為[未註冊裝置的受控應用程式新增應用程式](#)設定原則，以瞭解如何針對資料保護應用程式組態案例建立受控應用程式應用程式設定原則。建立設定之後，您可以將原則指派給使用者群組。

後續步驟

- [什麼是應用程式保護原則？](#)
- [Microsoft Intune 的應用程式組態原則](#)

使用iOS的Outlook和Android搭配 Microsoft Intune 來管理傳訊共同作業存取

2022/9/27 •

iOS和Android應用程式的Outlook是設計來讓組織中的使用者透過將電子郵件、行事曆、連絡人和其他檔案結合在一起，從其行動裝置執行更多動作。

當您訂閱包含Microsoft Intune和Azure Active Directory Premium功能的Enterprise Mobility + Security套件時，即可使用Microsoft 365資料最豐富且最廣泛的保護功能。例如條件式存取。您至少會想要部署條件式存取原則，以允許從行動裝置連線到iOS和Android Outlook，以及可確保共同作業體驗受到保護的Intune應用程式保護原則。

套用條件式存取

組織可以使用 Azure AD 條件式存取原則，以確保使用者只能使用iOS和Android的Outlook來存取公司或學校內容。若要這樣做，您需要以所有潛在使用者為目標的條件式存取原則。這些原則會在 [條件式存取:需要核准的用戶端應用程式或應用程式保護原則](#) 中說明。

1. 請遵循使用行動 [裝置要求核准的用戶端應用程式或應用程式保護原則](#) 中的步驟。此原則允許Outlook iOS和Android，但會封鎖能夠Exchange ActiveSync行動用戶端連線到Exchange Online的 OAuth 和基本驗證。

NOTE

此原則可確保行動使用者可以使用適用的應用程式存取所有Microsoft 365端點。

2. 請遵循 [封鎖所有裝置上的Exchange ActiveSync](#) 中的步驟，以防止Exchange ActiveSync在非行動裝置上使用基本驗證的用戶端連線到Exchange Online。

上述原則會利用授與存取控制[[需要應用程式保護原則](#)]，以確保在授與存取權之前，Intune應用程式保護原則會套用至iOS和Android Outlook內的相關聯帳戶。如果未將使用者指派給Intune應用程式保護原則、未獲得Intune的授權，或應用程式未包含在Intune應用程式保護原則中，則原則會防止使用者取得存取權杖並取得傳訊資料的存取權。

3. 請遵循 [如何:使用條件式存取封鎖對 Azure AD 的舊版驗證](#) 中的步驟，以封鎖iOS和Android裝置上其他Exchange通訊協定的舊版驗證;此原則僅應以Microsoft Exchange Online雲端應用程式和iOS和Android 裝置平臺。這可確保使用具有基本驗證Exchange Web 服務、IMAP4 或 POP3 通訊協定的行動應用程式無法連線到Exchange Online。

NOTE

若要利用以應用程式為基礎的條件式存取原則，Microsoft Authenticator應用程式必須安裝在iOS裝置上。針對Android裝置，需要Intune 公司入口網站應用程式。如需詳細資訊，請參閱使用[Intune的應用程式型條件式存取](#)。

建立Intune應用程式保護原則

應用程式保護原則 (APP) 定義允許哪些應用程式，以及它們可對組織資料採取的動作。APP 中可用的選項可讓組織根據其特定需求量身打造保護。對某些人而言，實作完整案例所需的原則設定可能不明顯。為了協助組織排定行動用戶端點強化的優先順序，Microsoft 已針對其應用程式資料保護架構引進分類法，以進行iOS和Android行動應用程式管理。

APP 資料保護架構會組織成三個不同的組態層級，每個層級會根據上一個層級來建置：

- Enterprise層級 1 (**基本資料保護**) 確保應用程式受到 PIN 保護並加密，並執行選擇性抹除作業。針對Android裝置，此層級會驗證Android裝置證明。這是一種進入層級設定，可在信箱原則Exchange Online提供類似的資料保護控制，並將 IT 和使用者母體引進 APP。
- Enterprise層級 2 (**增強的資料保護**) 引進 APP 資料外泄防護機制和最低作業系統需求。這是適用於大部分存取公司或學校資料之行動使用者的設定。
- Enterprise**高資料保護** (層級 3) 引進進階資料保護機制、增強的 PIN 設定，以及 APP Mobile Threat Defense。此設定適用於存取高風險資料的使用者。

若要查看每個設定層級的特定建議，以及必須保護的最低應用程式，請 [檢閱使用應用程式保護原則的資料保護架構](#)。

無論裝置是否已在統一端點管理 (UEM) 解決方案中註冊，都必須使用[如何建立和指派應用程式保護原則](#)中的步驟，為iOS和Android應用程式建立Intune應用程式保護原則。這些原則至少必須符合下列條件：

- 它們包含所有Microsoft 365行動應用程式，例如 Edge、Outlook、OneDrive、Office或Teams，因為這可確保使用者可以安全的方式存取及操作任何 Microsoft 應用程式內的工作或學校資料。
- 它們會指派給所有使用者。這可確保所有使用者都受到保護，無論他們使用Outlook來進行iOS或Android。
- 判斷哪個架構層級符合您的需求。大部分的組織都應該實作 Enterprise**增強型資料保護** (層級 2) 中定義的設定，以啟用資料保護和存取需求控制。

如需可用設定的詳細資訊，請[參閱Android應用程式保護原則設定](#)和[iOS應用程式保護原則設定](#)。

IMPORTANT

若要對未在 Intune 中註冊的Android裝置上套用Intune應用程式保護原則，使用者也必須安裝Intune 公司入口網站。

使用應用程式設定

iOS和Android的Outlook支援允許統一端點管理的應用程式設定，例如Microsoft 端點管理員，系統管理員可自訂應用程式的行為。

應用程式設定可以透過已註冊裝置上的行動裝置管理 (MDM) OS 通道，(iOS的受控[應用程式組態](#)通道，或Android) Enterprise通道中的Android，或透過 Intune App Protection 原則 (APP) 通道來傳遞。iOS和Android 的Outlook支援下列組態案例：

- 只允許公司或學校帳戶
- 一般應用程式組態設定
- S/MIME 設定
- 資料保護設定

如需iOS和Android支援的應用程式組態設定Outlook的特定程式步驟和詳細檔，請參閱[部署iOS和Android應用程式組態設定的Outlook](#)。

後續步驟

- [什麼是應用程式保護原則？](#)
- [Microsoft Intune 的應用程式組態原則](#)

使用 Microsoft Intune 管理 iOS 和 Android Teams 中的共同作業體驗

2022/9/27 •

Microsoft Teams 是小組在 Microsoft 365 中共同作業的中樞，可整合小組需要更投入且更有效率的人員、內容和工具。

當您訂閱包含 Microsoft Intune 和 Azure Active Directory Premium 功能的 Enterprise Mobility + Security 套件時，即可使用 Microsoft 365 資料最豐富且最廣泛的保護功能。例如條件式存取。您至少會想要部署條件式存取原則，以允許從行動裝置連線至 iOS 和 Android Teams，以及可確保共同作業體驗受到保護的 Intune 應用程式保護原則。

套用條件式存取

組織可以使用 Azure AD 條件式存取原則，確保使用者只能使用 iOS 和 Android 的 Teams 來存取公司或學校內容。若要這樣做，您需要以所有潛在使用者為目標的條件式存取原則。這些原則會在 [條件式存取：需要核准的用戶端應用程式或應用程式保護原則](#) 中說明。

NOTE

若要利用以應用程式為基礎的條件式存取原則，Microsoft Authenticator 應用程式必須安裝在 iOS 裝置上。針對 Android 裝置，需要 Intune 公司入口網站應用程式。如需詳細資訊，請參閱使用 [Intune 的應用程式型條件式存取](#)。

請遵循使用行動 [裝置要求核准的用戶端應用程式或應用程式保護原則](#) 中的步驟，這會允許 iOS 和 Android 的 Teams，但會封鎖協力廠商支援 OAuth 的行動裝置用戶端連線到 Microsoft 365 端點。

NOTE

此原則可確保行動使用者可以使用適用的應用程式存取所有 Microsoft 365 端點。

建立 Intune 應用程式保護原則

應用程式保護原則 (APP) 定義允許哪些應用程式，以及它們可對組織資料採取的動作。APP 中可用的選項可讓組織根據其特定需求量身打造保護。對某些人而言，實作完整案例所需的原則設定可能不明顯。為了協助組織排定行動用戶端點強化的優先順序，Microsoft 已針對其應用程式資料保護架構引進分類法，以進行 iOS 和 Android 行動應用程式管理。

APP 資料保護架構會組織成三個不同的組態層級，每個層級會根據上一個層級來建置：

- Enterprise 層級 1 (**基本資料保護**) 確保應用程式受到 PIN 保護並加密，並執行選擇性抹除作業。針對 Android 裝置，此層級會驗證 Android 裝置證明。這是一種進入層級設定，可在信箱原則 Exchange Online 提供類似的資料保護控制，並將 IT 和使用者母體引進 APP。
- Enterprise 層級 2 (**增強的資料保護**) 引進 APP 資料外泄防護機制和最低作業系統需求。這是適用於大部分存取公司或學校資料之行動使用者的設定。
- Enterprise 高資料保護 (層級 3) 引進進階資料保護機制、增強的 PIN 設定，以及 APP Mobile Threat Defense。此設定適用於存取高風險資料的使用者。

若要查看每個設定層級的特定建議，以及必須保護的最低應用程式，請 [檢閱使用應用程式保護原則的資料保護架構](#)。

無論裝置是否已在統一端點管理 (UEM) 解決方案中註冊，都必須使用[如何建立和指派應用程式保護原則](#)中的步驟，為iOS和Android應用程式建立Intune應用程式保護原則。這些原則至少必須符合下列條件：

1. 它們包含所有Microsoft 365行動應用程式，例如 Edge、Outlook、OneDrive、Office或Teams，因為這可確保使用者可以安全的方式存取及操作任何 Microsoft 應用程式內的工作或學校資料。
2. 它們會指派給所有使用者。這可確保所有使用者都受到保護，不論他們使用Teams進行iOS還是Android。
3. 判斷哪個架構層級符合您的需求。大部分的組織都應該實作 Enterprise增強型資料保護 (層級 2) 中定義的設定，以啟用資料保護和存取需求控制。

如需可用設定的詳細資訊，請參閱[Android應用程式保護原則設定](#)和[iOS應用程式保護原則設定](#)。

IMPORTANT

若要對未在Intune中註冊的Android裝置上套用Intune應用程式保護原則，使用者也必須安裝Intune 公司入口網站。

利用應用程式設定

iOS和Android的Teams支援允許統一端點管理的應用程式設定，例如Microsoft 端點管理員系統管理員自訂應用程式的行為。

應用程式設定可以透過已註冊裝置上的行動裝置管理 (MDM) OS 通道，(iOS的受控[應用程式組態](#)通道，或Android) Enterprise通道中的Android，或透過 Intune App Protection 原則 (APP) 通道來傳遞。iOS和Android的Teams支援下列組態案例：

- 只允許公司或學校帳戶

IMPORTANT

針對需要在Android上註冊裝置的組態案例，裝置必須在Android Enterprise中註冊，而Android的Teams必須透過受控Google Play存放區進行部署。如需詳細資訊，請參閱[設定Android Enterprise個人擁有工作設定檔裝置的註冊](#)和[新增受控Android Enterprise裝置的應用程式設定原則](#)。

每個組態案例都會強調其特定需求。例如，設定案例是否需要裝置註冊，因此可與任何 UEM 提供者搭配使用，或需要Intune應用程式保護原則。

IMPORTANT

應用程式設定金鑰會區分大小寫。使用適當的大小寫以確保設定生效。

NOTE

透過Microsoft 端點管理員，透過 MDM OS 通道傳遞的應用程式設定稱為受控  應用程式組態原則 (ACP) ;透過應用程式保護原則通道傳遞的應用程式設定稱為受控  應用程式組態原則。

只允許公司或學校帳戶

遵守我們最大且高度管制客戶的資料安全性與合規性原則，是Microsoft 365價值的重要要素。有些公司需要擷取其公司環境中的所有通訊資訊，以及確保裝置僅用於公司通訊。若要支援這些需求，Teams在已註冊裝置上iOS和Android可以設定為只允許在應用程式內布建單一公司帳戶。

您可以在這裡深入瞭解如何設定組織允許的帳戶模式設定：

- [Android設定](#)
- [iOS設定](#)

此設定案例僅適用於已註冊的裝置。不過，支援任何 UEM 提供者。如果您不是使用Microsoft 端點管理員，則必須參閱 UEM 檔，以瞭解如何部署這些組態金鑰。

後續步驟

- [什麼是應用程式保護原則？](#)
- [Microsoft Intune 的應用程式組態原則](#)

使用 Intune 設定適用於 Android 裝置的 Google Chrome

2022/9/27 •

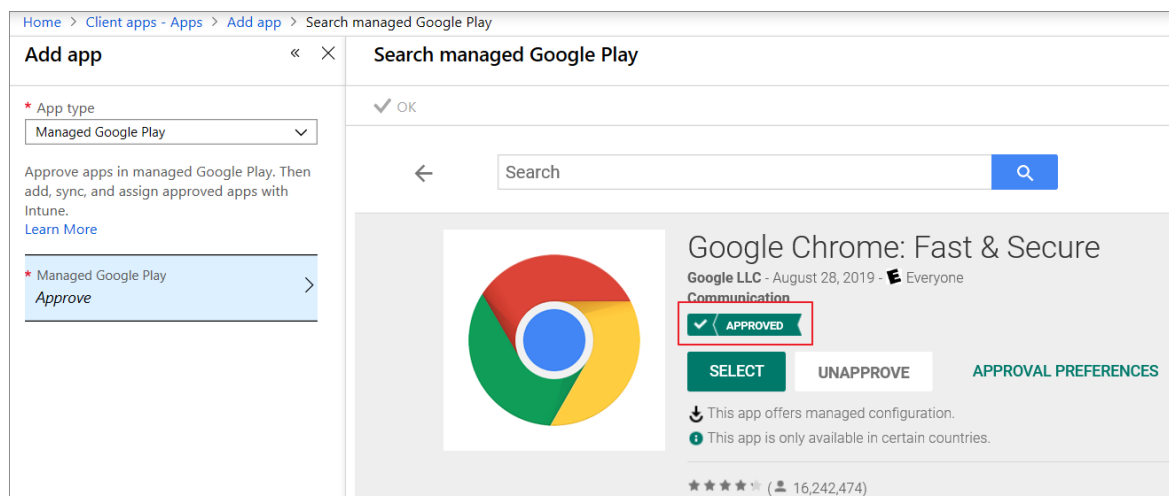
您可以使用Intune應用程式設定原則來設定適用於 Android 裝置的 Google Chrome。應用程式的設定可以自動套用。例如，您可以特別設定要封鎖或允許的書籤和 URL。

先決條件

- 使用者的 Android Enterprise 裝置必須在Intune中註冊。如需詳細資訊，[請參閱設定 Android Enterprise 個人擁有工作設定檔裝置的註冊](#)。
- Google Chrome 會新增為受控 Google Play 應用程式。如需受控 Google Play 的詳細資訊，請參閱[將您的 Intune帳戶連線到受控 Google Play 帳戶](#)。

將 Google Chrome 應用程式新增至 Intune

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有 > 應用程式 >] [新增]，然後新增受控 Google Play 應用程式。
3. 移至受控 Google Play，使用 Google Chrome 進行搜尋並核准。



4. 將 Google Chrome 指派給群組作為必要的應用程式類型。當裝置註冊到Intune時，將會自動部署 Google Chrome。

如需將受控 Google Play 應用程式新增至 Intune 的其他詳細資料，請參閱[受控 Google Play 商店應用程式](#)。

新增受控 AE 裝置的應用程式設定

1. 從 [Microsoft 端點管理員系統管理中心](#)，選取 [應用程式 > 應用程式設定原則 >] [新增 > 受控裝置]。
2. 設定下列詳細資料：
 - 名稱 - 出現在入口網站中的設定檔名稱。
 - 描述 - 顯示在入口網站中的設定檔描述。
 - 裝置註冊類型 - 此設定設為受控裝置。
 - 平臺 - 選取 [Android]。

Add configuration policy

* Name ⓘ
Google Chrome Configuration ✓

Description ⓘ
Enter a description...

* Device enrollment type ⓘ
Managed devices ▼

* Platform ⓘ
Android ▼

3. 按一下 [相關聯的應用程式] 以顯示 [相關聯的應用程式] 窗格。尋找並選取 [Google Chrome]。此清單包含您已核准並與Intune同步處理的受控 Google Play 應用程式。

Add configuration policy

* Name ⓘ
Google Chrome Configuration ✓

Description ⓘ
Enter a description...

* Device enrollment type ⓘ
Managed devices ▼

* Platform ⓘ
Android ▼

Scope (Tags)
0 scope(s) selected >

Associated app ⓘ
Select the required app >

Associated app

Google Chrome Configuration

Search by name or publisher...

NAME	PUBLISHER	TYPE
Box	Box	Managed Google Play app
Google Chrome: Fast & Secure	Google LLC	Managed Google Play app
Managed Home Screen	Microsoft Corporation	Managed Google Play app
Microsoft Authenticator	Microsoft Corporation	Managed Google Play app
Microsoft OneDrive	Microsoft Corporation	Managed Google Play app
Microsoft OneNote: Save Ideas and Organ...	Microsoft Corporation	Managed Google Play app
Microsoft Outlook	Microsoft Corporation	Managed Google Play app

4. 按一下 [組態設定]，選取 [使用設定設計 工具]，然後按一下 [新增] 以選取組態金鑰。

Use the JSON editor to configure the disabled configuration keys.

Configuration settings format ⓘ Use configuration designer ▼

Add

CONFIGURATION KEY	VALUE TYPE	CONFIGURATION VALUE	DESCRIPTION

以下是常見設定的範例：

- 封鎖對 URL 清單的存取: ["*"]
- 允許存取 URL 清單: ["baidu.com", "youtube.com", "chromium.org", "chrome://*"]
- Managed 書籤:

```
[{"toplevel_name": "My managed bookmarks folder" }, {"url": "baidu.com", "name": "Baidu"}, {"url": "youtube.com", "name": "Youtube"}, {"name": "Chrome links", "children": [{"url": "chromium.org", "name": "Chromium"}, {"url": "dev.chromium.org", "name": "Chromium Developers"}]}
```

- Incognito 模式可用性: Incognito mode disabled

使用組態設計工具新增組態設定之後，它們會列在資料表中。

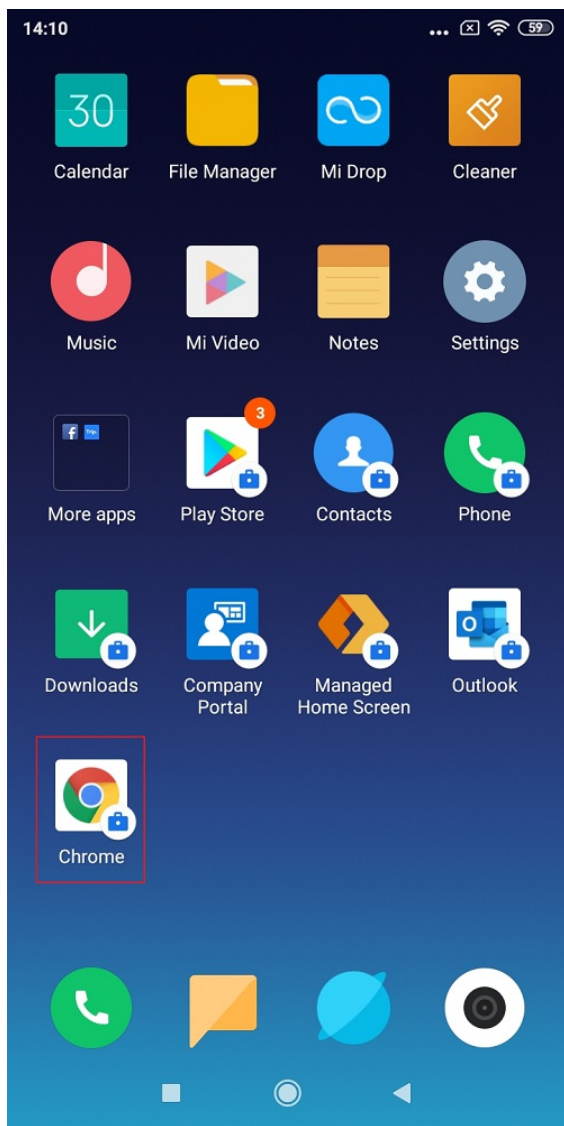
Configuration settings format ⓘ Use configuration designer ▼			
Add			
CONFIGURATION KEY	VALUE TYPE	CONFIGURATION VALUE	DESCRIPTION
Managed Bookmarks	string	[{"toplevel_name": "My ma...	Configures a list of managed book...
Block access to a list of URLs	string	["*"]	This policy prevents the user from ...
Incognito mode availability	choice	1	Specifies whether the user may op...
Allow access to a list of URLs	string	["baidu.com", "yahoo.com", ...	Allows access to the listed URLs, a...

上述設定會建立書籤，並封鎖對、`yahoo.com`、`chromium.org` 和 `chrome://` 以外的 `baidu.com` 所有 URL 的存取。

5. 按一下 [確定] 和 [新增]，將您的設定原則新增至Intune。
6. 將此設定原則指派給使用者群組。如需詳細資訊，[請參閱使用 Microsoft Intune 將應用程式指派給群組。](#)

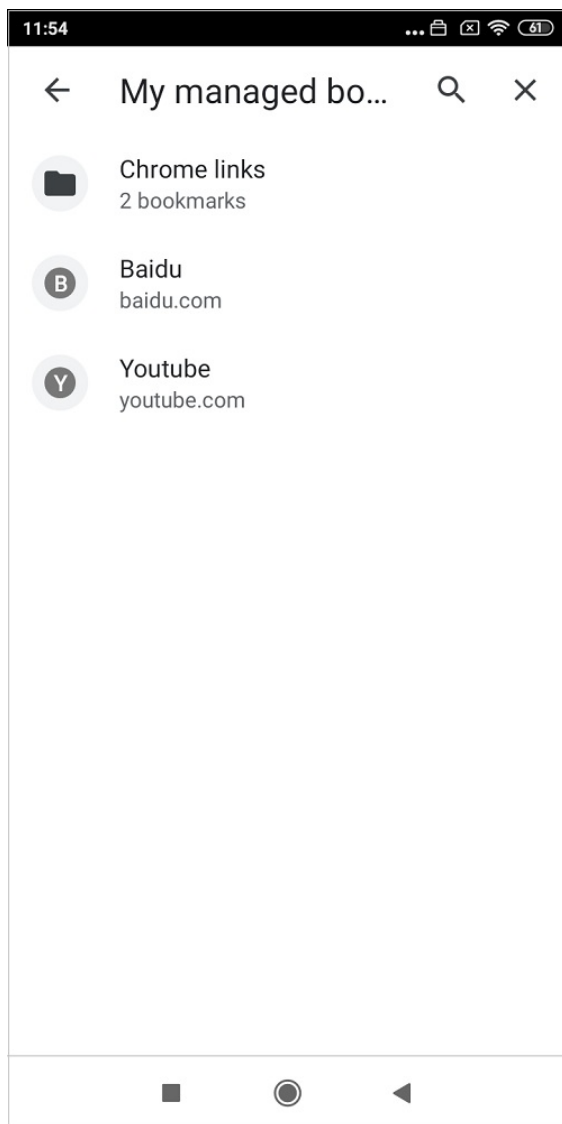
確認裝置設定

向 Android Enterprise 註冊 Android 裝置之後，將會自動部署具有公事包圖示的受控 Google Chrome 應用程式。

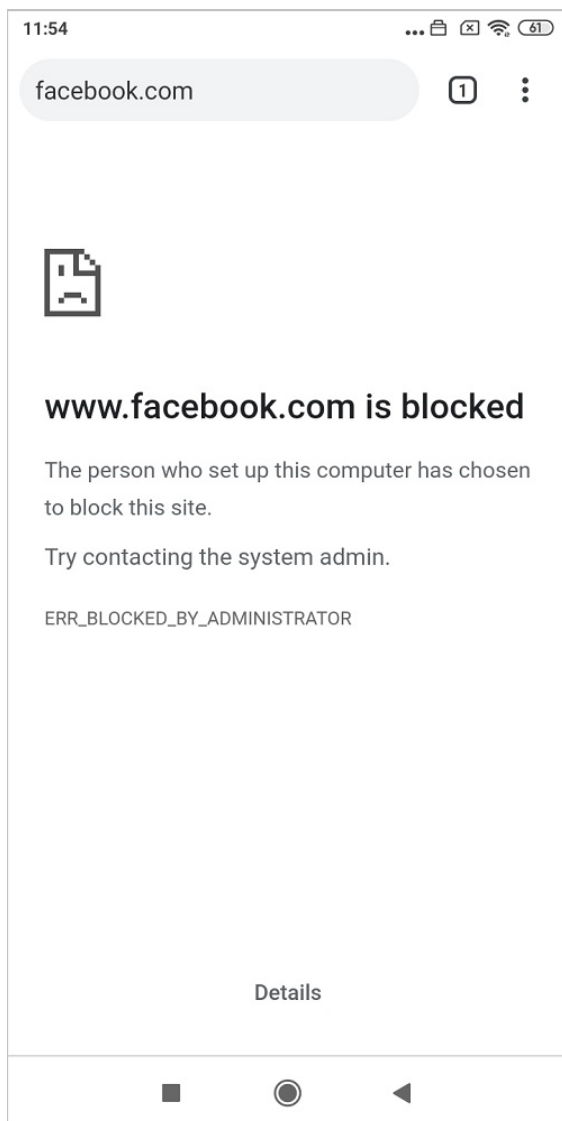


啟動 Google Chrome, 您會發現已套用設定。

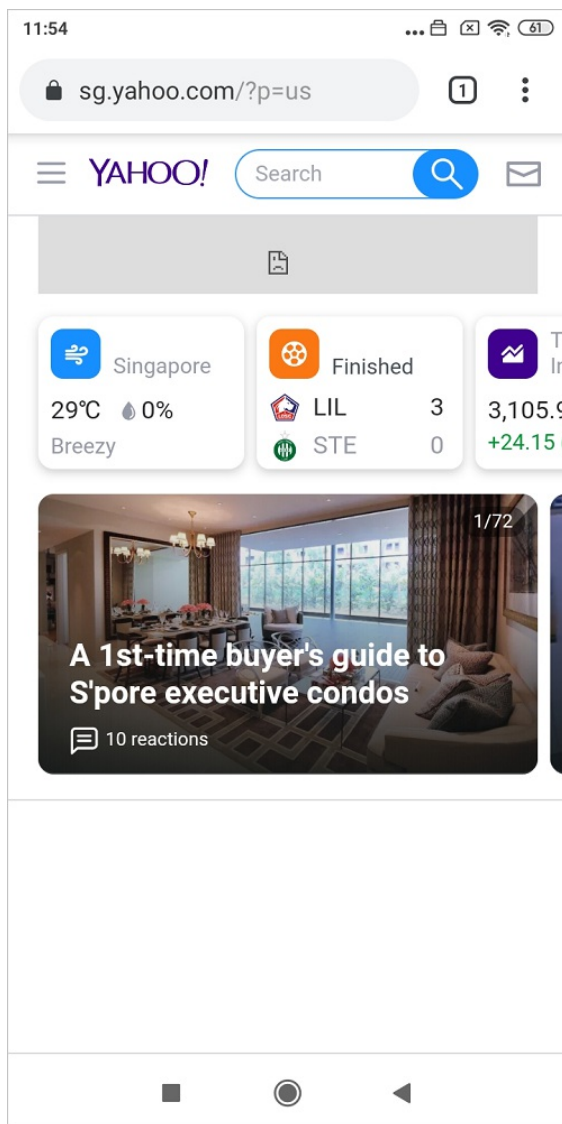
書籤:



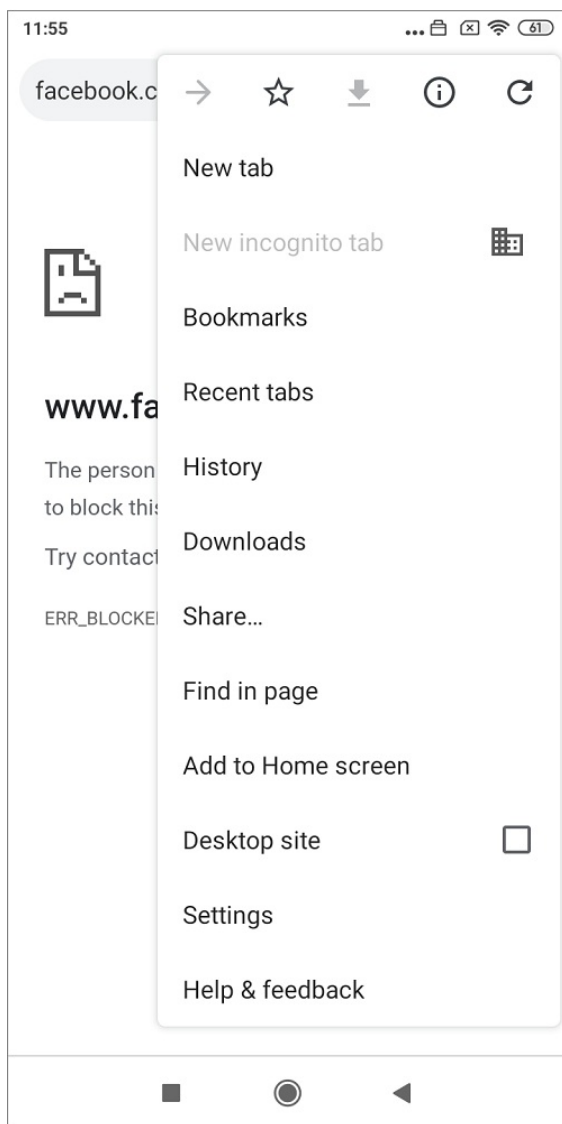
封鎖的 URL:



允許 URL：



Incognito 索引標籤:

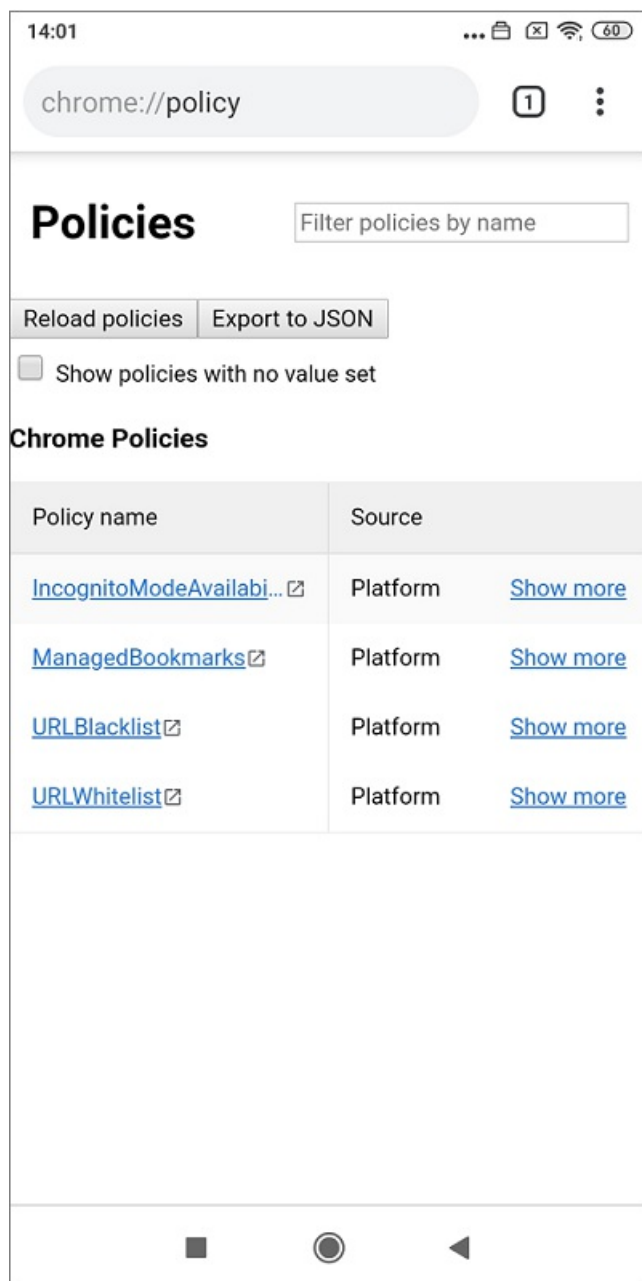


疑難排解

1. 檢查Intune以監視原則部署狀態。

Chrome Configuration - Device install status			
Search (Ctrl+/) Export Filter			
Filter items...			
DEVICE NAME	USER NAME	STATUS	LAST CHECK-IN
afw_AndroidForWork_9/4/2019_4:00 AM	afw@contoso.onmicrosoft.com	Succeeded	9/04/19, 1:53 PM

2. 啟動 Google Chrome 並流覽 `chrome://policy`。我們可以確認設定是否已成功套用。



其他資訊

- [新增受控 Android Enterprise 裝置的應用程式設定原則](#)
- [Chrome Enterprise 原則清單](#)

後續步驟

- 如需 Android Enterprise 完全受控裝置的詳細資訊，請參閱[設定 Android Enterprise 完全管理裝置的Intune註冊](#)。

在 Microsoft Intune 中使用 Android Enterprise 裝置上的 vpn 和每個應用程式 vpn 原則

2022/9/27 •

虛擬私人網路 (VPN) 可讓使用者從遠端存取組織資源，包括在家、酒店、cafes 等。在 Microsoft Intune 中，您可以使用 app configuration 原則，在 Android Enterprise 裝置上設定 VPN 用戶端應用程式。然後，將此原則與其 VPN 設定部署至組織中的裝置。

您也可以建立特定應用程式所使用的 VPN 原則。這項功能稱為「每個應用程式 VPN」。當應用程式使用中時，它可以連線至 VPN，並透過 VPN 存取資源。當應用程式不在使用中時，不會使用 VPN。

本功能適用於：

- Android 企業版

為 VPN 用戶端應用程式建立應用程式設定原則的方法有兩種：

- 設定設計工具
- JSON 資料

本文說明如何使用這兩個選項來建立每個應用程式 VPN 和 VPN 應用程式佈建原則。

NOTE

許多 VPN 用戶端設定參數類似。不過，每個應用程式都有其唯一的金鑰和選項。如有任何問題，請與您的 VPN 廠商聯繫。

開始之前

- 當應用程式開啟時，Android 不會自動觸發 VPN 用戶端連線。必須手動啟動 VPN 連線。或者，您可以使用 [always-ON VPN](#) 來啟動連接。
- 下列 VPN 用戶端支援 Intune 的應用程式佈建原則：
 - Cisco AnyConnect
 - Citrix SSO
 - F5 存取
 - Palo Alto 網路 GlobalProtect
 - 脈衝安全
 - SonicWall 行動裝置連線
- 當您在 Intune 中建立 VPN 原則時，您會選取不同的金鑰加以設定。這些金鑰名稱會因不同的 VPN 用戶端應用程式而有所不同。所以，您環境中的主要名稱可能會不同于本文中的範例。
- 設定設計工具和 JSON 資料可成功使用憑證型驗證。如果 VPN 驗證需要用戶端憑證，請先建立憑證設定檔，再建立 VPN 原則。VPN 應用程式佈建原則使用來自憑證設定檔的值。

Android Enterprise 個人擁有的工作設定檔裝置支援 SCEP 和 PKCS 憑證。Android Enterprise 完全管理、專用及公司擁有的工作設定檔裝置只支援 SCEP 憑證。如需詳細資訊，請參閱在 [Microsoft Intune 使用憑證以進行驗證](#)。

每個應用程式 VPN 概述

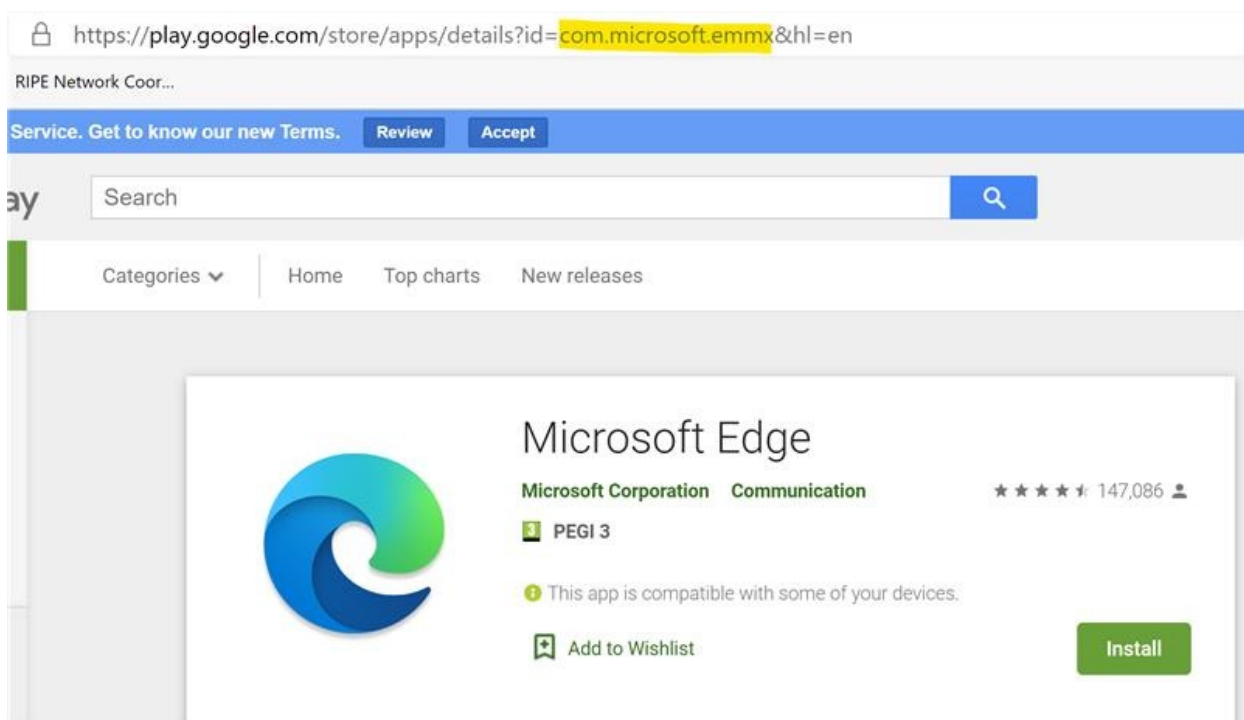
當您建立及測試每個應用程式的 VPN 時，基本流程包含下列步驟：

1. 選取 VPN 用戶端應用程式。在本文中 ([開始之前](#)) 列出支援的應用程式。
2. 取得將使用 VPN 連線之應用程式的應用程式套件 IDs。取得此篇文章中 ([的應用程式套件識別碼](#)) 會向您說明方式。
3. 如果您使用憑證來驗證 VPN 連線，請先建立並部署憑證設定檔，再部署 VPN 原則。請確定已成功部署憑證設定檔。如需詳細資訊，請參閱在 [Microsoft Intune 使用憑證以進行驗證](#)。
4. 將 [VPN 用戶端應用程式](#) 新增至 Intune，並將應用程式部署至您的使用者和裝置。
5. 建立 VPN 應用程式佈建原則。使用原則中的應用程式套件 IDs 和憑證資訊。
6. 部署新的 VPN 原則。
7. 確認 VPN 用戶端應用程式已順利連接至您的 VPN 伺服器。
8. 當應用程式處於使用中狀態時，請確認您應用程式的流量順利透過 VPN。

取得應用程式套件識別碼

取得將使用 VPN 之每個應用程式的套件識別碼。針對公開提供的應用程式，您可以在 Google Play store 中取得應用程式套件識別碼。每個應用程式的顯示 URL 包含套件識別碼。

在下列範例中，Microsoft Edge 瀏覽器應用程式的套件識別碼是 `com.microsoft.emmx`。套件識別碼屬於 URL：



若為商務用 (LOB) 應用程式，請從廠商或應用程式開發人員取得套件識別碼。

憑證

本文假設您的 VPN 連線使用憑證型驗證。它也會假設您已成功部署用戶端成功驗證所需鏈中的所有憑證。一般來說，此憑證鏈包含用戶端憑證、任何中級憑證和根憑證。

如需憑證的詳細資訊，請參閱在 [Microsoft Intune 使用憑證以進行驗證](#)。

當您的用戶端驗證憑證設定檔部署時，它會在憑證設定檔中建立憑證權杖。此 token 是用來建立 VPN 應用程式設定原則。

如果您不熟悉如何建立應用程式設定原則，請參閱 [為受管理的 Android Enterprise 裝置新增應用程式佈建原則](#)。

使用設定設計工具

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 **應用 > 程式的應用程式設定原則 > 新增 > 受管理裝置**。
3. 在 [基本資訊] 中，輸入下列內容：
 - **名稱**：輸入原則的描述性名稱。為您的設定檔命名，以方便之後能夠輕鬆識別。例如，良好的原則名稱是 **應用程式設定原則：Cisco AnyConnect Android 的 VPN 原則 Enterprise 工作設定檔裝置**。
 - **描述**：輸入原則的描述。這是選擇性設定，但建議進行。
 - **Platform**：選取 **Android Enterprise**。
 - **配置檔案類型**：您的選項：
 - **所有配置檔案類型**：此選項支援使用者名稱和密碼驗證。如果您使用憑證型驗證，請勿使用此選項。
 - **完全受管理、專用及 Corporate-Owned 的工作設定檔**：此選項支援憑證型驗證，以及使用者名稱和密碼驗證。
 - **僅限個人擁有的工作設定檔**：此選項支援憑證型驗證，以及使用者名稱和密碼驗證。
 - **目標應用程式**：選取您先前新增的 VPN 用戶端應用程式。在下列範例中，會使用 Cisco AnyConnect VPN 用戶端應用程式：

Create app configuration policy

1 Basics2 Settings3 Assignments4 Review + create

Name *

AE WP AC VPN

✓

Description

Android Enterprise Work Profile AnyConnect VPN

✓

Device enrollment type

Managed devices

▼

Platform * ⓘ

Android Enterprise

▼

Profile Type * ⓘ

Work Profile Only

▼

Targeted app * ⓘ



4. 選取 [下一步]。
5. 在 **設定** 中，輸入下列屬性：
 - **配置設定格式**：選取 [使用設定設計 工具]：

Create app configuration policy

✓ Basics **2 Settings** ③ Assignments ④ Review + create

Permissions

Permissions granted here will override the "Default app permissions" policy for the selected apps.

[Learn more about Android runtime permissions](#)

+Add

Not configured

Configuration Settings

Configuration settings format ①

Use configuration designer



Use the JSON editor to configure the disabled configuration keys.

+Add

Not configured

- **Add**: 顯示設定機碼清單。選取您設定所需的所有設定機碼 > 確定。

在下列範例中，我們為 AnyConnect VPN 選取最小清單，包括憑證型驗證及每個應用程式 VPN：

 Use the JSON editor to configure the disabled configuration keys.

 Search to filter items...			
☐	Configuration k... ↑↓	Value type	↑↓ Descripti
☒	Connection Name	string	User frier
☒	Host	string	URL to th
☒	Protocol	choice	VPN tunr
☐	IPsec Authentication...	choice	(Optional
☐	IKE identity	string	(Optional
☒	KeyChain Certificate ...	string	(Optional
☐	Per App VPN Allowe...	string	(Depreca
☒	Per App VPN Allowe...	string	(Optional
☐	Per App VPN Disallo...	string	(Optional
☐	Allow Apps to Bypas...	bool	(Optional

- **設定 值**: 輸入您所選取之設定機碼的值。請記住, 主要名稱會根據您所使用的 VPN 用戶端應用程式而有所不同。在範例中選取的按鍵中:

- **每個應用程式 VPN 允許的應用 程式**: 輸入您先前收集的應用程式套件識別碼(s)。例如:

Per App VPN Allowed Ap...	string	com.microsoft.emmx	(Optional)- Specifies which app... ***

- **金鑰鏈憑證別名 (選用)**: 將 數值型別 從 字串 變更為 憑證。選取要搭配 VPN 驗證使用的用戶端憑證設定檔。例如:

KeyChain Certificate Alias	certificate	AE-WP-SCEP	(Optional)- KeyChain alias of th... ***

- **通訊協定**: 選取 VPN 的 SSL 或 IPsec 隧道通訊協定。
- **連接名稱**: 輸入 VPN 連線的使用者易記名稱。使用者在其裝置上看到此連線名稱。例如, enter `ContosoVPN`。
- **主機**: 輸入頭端路由器的主機名稱 URL。例如, enter `vpn.contoso.com`。

Protocol	choice	IPsec	VPN tunnel protocol (SSL or IPs... ***
Host	string	vpn.contoso.com	URL to the headend. This field i... ***
Connection Name	string	ContosoVPN ✓	User friendly name (for display ... ***

6. 選取 [下一步]。

7. 在 [工作分派] 中，選取要指派 VPN 應用程式佈建原則的群組。

選取 ****[下一步]。

8. 在 [檢閱 + 建立] 中，檢閱您的設定。當您選取 [建立] 時，就會儲存您的變更，並將原則部署至您的群組。原則也會顯示在 [應用程式佈建原則] 清單中。

Create app configuration policy

✓ Basics
✓ Settings
✓ Assignments
4 Review + create

Summary

Basics

Name	AE WP AC VPN
Description	Android Enterprise Work Profile AnyConnect VPN
Device enrollment type	Managed devices
Platform	Android Enterprise
Profile Type	Work Profile Only
Targeted app	AnyConnect

Settings

Permissions

Not configured

Configuration Settings

Configuration key	Value type	Configuration value
KeyChain Certificate Alias	certificate	{{cert:a5280c11-91a9-4f5e-8fa6-5e5cd5...
Per App VPN Allowed Apps	string	com.microsoft.emmx
Protocol	choice	IPsec
Host	string	vpn.contoso.com
Connection Name	string	ContosoVPN

Assignments

Included groups	All users All devices
Excluded groups	--

使用 JSON

如果您沒有使用此選項，或不知道設定 設計 工具中所用的所有必要 VPN 設定，請使用此選項。如需協助，請與您的 VPN 廠商聯繫。

取得憑證 token

在這些步驟中，建立暫時原則。不會儲存原則。目的是要複製憑證權杖。使用 JSON (下一節) 中建立 VPN 原則時，您將使用此權杖。

1. 在 [Microsoft 端點管理員系統管理中心](#)，選取 [應用 > 程式應用程式設定原則 >] [新增 > 受管理的裝置]。
2. 在 [基本資訊] 中，輸入下列內容：
 - 名稱：輸入任何名稱。這個原則為暫時的，不會儲存。
 - Platform：選取 Android Enterprise。
 - 配置檔案類型：僅選取 [僅限個人擁有的工作設定檔]。
 - 目標應用程式：選取您先前新增的 VPN 用戶端應用程式。
3. 選取 [下一步]。
4. 在 設定 中，輸入下列屬性：
 - 配置設定格式：選取 [使用設定設計 工具]。
 - Add：顯示設定機碼清單。選取 數值型別 為 string 的任何索引鍵。選取 [確定]。

 Use the JSON editor to configure the disabled configuration keys.

Search to filter items...

×

Configuration k... ↑↓

Value type

↑↓

Descripti

Connection Name

string

User frier

Host

string

URL to th

Protocol

choice

VPN tunr

5. 將 數值型別 從 字串 變更為 憑證。這個步驟可讓您選取正確的用戶端憑證設定檔，以驗證 VPN：

Configuration key	Value type	Configuration value	Description
Connection Name	certificate	AE-DO-SCEP	User friendly name (for display ... ***

6. 立即將 數值型別 變更回 string。設定 值 變更為 token `{{cert:GUID}}`：

Configuration key	Value type	Configuration value	Description
Connection Name	string	{{cert:7153cb3b-3929-4d...	User friendly name (for display ... ***

7. 將此憑證權杖複製並貼到另一個檔案，例如文字編輯器。
8. 捨棄此原則。請勿儲存。唯一的目的是複製並貼上憑證權杖。

使用 JSON 建立 VPN 原則

1. 在 [Microsoft 端點管理員系統管理中心](#)，選取 [應用 > 程式應用程式設定原則 >] [新增 > 受管理的裝置]。
2. 在 [基本資訊] 中，輸入下列內容：

- **名稱**：輸入原則的描述性名稱。為您的設定檔命名，以方便之後能夠輕鬆識別。例如，好的原則名稱是應用程式設定原則：JSON Cisco AnyConnect VPN 原則 for Android Enterprise 整個公司的工作設定檔裝置。
- **描述**：輸入原則的描述。這是選擇性設定，但建議進行。
- **Platform**：選取 Android Enterprise。
- **配置檔案類型**：您的選項：
 - **所有配置檔案類型**：此選項支援使用者名稱和密碼驗證。如果您使用憑證型驗證，請勿使用此選項。
 - **完全受管理、專用及 Corporate-Owned 的工作設定檔**：此選項支援憑證型驗證，以及使用者名稱和密碼驗證。
 - **僅限個人擁有的工作設定檔**：此選項支援憑證型驗證，以及使用者名稱和密碼驗證。
- **目標應用程式**：選取您先前新增的 VPN 用戶端應用程式。

3. 選取 [下一步]。

4. 在 **設定** 中，輸入下列屬性：

- **設定設定格式**：選取 [輸入 JSON 資料]。您可以直接編輯 JSON。
- **下載 JSON 範本**：使用此選項可下載和更新任何外部編輯器中的範本。請小心使用 Smart 引號 的文字編輯器，因為它們可能會建立不正確 JSON。

在您輸入設定所需的值後，請移除所有或 `STRING_VALUE` 的 `"STRING_VALUE"` 設定。

Create app configuration policy

✓ Basics 2 Settings 3 Assignments 4 Review + create

Permissions

Permissions granted here will override the "Default app permissions" policy for the selected apps.

[Learn more about Android runtime permissions](#)

+Add

Not configured

Configuration Settings

Configuration settings format ⓘ

Enter JSON data

Download JSON template

```

1  {
2      "kind": "androidenterprise#managedConfiguration",
3      "productId": "app:com.cisco.anyconnect.vpn.android.avf",
4      "managedProperty": [
5          {
6              "key": "vpn_connection_name",
7              "valueString": "ContosoVPN"
8          },
9          {
10             "key": "vpn_connection_host",
11             "valueString": "vpn.contoso.com"
12          },
13          {
14             "key": "vpn_connection_protocol",
15             "valueString": "IPsec"
16          },
17          {
18             "key": "vpn_connection_keychain_cert_alias",
19             "valueString": "{cert:7153cb3b-3929-4da3-b726-f9a8bf599734}"
20          },
21      ]
  
```

5. 選取 [下一步]。

6. 在 [工作分派] 中，選取要指派 VPN 應用程式佈建原則的群組。

選取 ****[下一步]。

7. 在 [檢閱 + 建立] 中，檢閱您的設定。當您選取 [建立] 時，就會儲存您的變更，並將原則部署至您的群組。原則也會顯示在 [應用程式佈建原則] 清單中。

F5 Access VPN 的 JSON 範例

```
{
  "kind": "androidenterprise#managedConfiguration",
  "productId": "app:com.f5.edge.client_ics",
  "managedProperty": [
    {
      "key": "disallowUserConfig",
      "valueBool": false
    },
    {
      "key": "vpnConfigurations",
      "valueBundleArray": [
        {
          "managedProperty": [
            {
              "key": "name",
              "valueString": "MyCorpVPN"
            },
            {
              "key": "server",
              "valueString": "vpn.contoso.com"
            },
            {
              "key": "webloginMode",
              "valueBool": false
            },
            {
              "key": "fipsMode",
              "valueBool": false
            },
            {
              "key": "clientCertKeychainAlias",
              "valueString": "{{cert:77333880-14e9-0aa0-9b2c-a1bc6b913829}}"
            },
            {
              "key": "allowedApps",
              "valueString": "com.microsoft.emmx"
            },
            {
              "key": "mdmAssignedId",
              "valueString": ""
            },
            {
              "key": "mdmInstanceId",
              "valueString": ""
            },
            {
              "key": "mdmDeviceUniqueId",
              "valueString": ""
            },
            {
              "key": "mdmDeviceWifiMacAddress",
              "valueString": ""
            },
            {
              "key": "mdmDeviceSerialNumber",
              "valueString": ""
            },
            {
              "key": "allowBypass",
```

```
}
    "valueBool": false
  }
]
}
```

其他資訊

- [新增受管理的 Android Enterprise 裝置的應用程式設定原則](#)
- [設定 Intune 中 VPN 的 Android Enterprise 裝置設定](#)

後續步驟

- [在 Intune 中建立 VPN 設定檔以連接至 VPN 伺服器](#)

使用 Microsoft Intune 管理大量購買的應用程式和手冊

2022/9/27 •

簡介

某些應用程式存放區可讓您購買您想要在公司中使用之應用程式或圖書的多個授權。大量購買授權可協助您減少追蹤多個已購買的應用程式和圖書副本的管理負荷。

Microsoft Intune 可協助您管理透過此程式所購買的應用程式和圖書。您從儲存區匯入授權資訊，並追蹤您使用的授權數目。此程式可協助確保您未安裝超過您擁有的應用程式或工作手冊複本。

您可以管理哪些類型的應用程式和圖書？

透過 Intune，您可以從 iOS 儲存區中管理您從該卷購買的應用程式和圖書，以及管理您從商務用 Microsoft Store 購買的應用程式。若要瞭解如何從每個儲存區管理授權的應用程式，請選擇下列其中一個主題：

- [管理 iOS/iPadOS 大量購買的應用程式](#)
- [從商務用 Microsoft Store 管理大量購買的應用程式](#)
- [如何管理 iOS/iPadOS eBooks](#)

如何使用 Microsoft Intune 管理透過 Apple Business Manager 購買的 iOS 和 macOS 應用程式

2022/9/27 •

Apple 讓您使用 [Apple Business Manager](#) 或 [Apple School Manager](#)，針對您想要在組織中用於 iOS/iPadOS 和 macOS 裝置上的應用程式購買多個授權。您可以將您的大量採購資訊與 Intune 同步處理，並追蹤大量採購的應用程式使用情況。購買應用程式授權可協助您有效地管理公司內的應用程式，並保留對已購買之應用程式的擁有權和控制。

Microsoft Intune 可藉由下列方式協助您管理透過此方案所購買的應用程式：

- 同步您從 Apple Business Manager 所下載的位置權杖。
- 追蹤有多少已購買的應用程式可供使用及已經使用。
- 協助您安裝所擁有之最大授權數量的應用程式。

此外，針對從 Apple Business Manager 所購買的書籍，您可以使用 Intune 來針對 iOS/iPadOS 裝置進行同步處理、管理及指派。如需詳細資訊，請參閱[如何管理透過大量採購方案購買的 iOS/iPadOS 電子書](#)。

什麼是位置權杖？

位置權杖是大量採購授權，以前稱為大量採購方案 (VPP) 權杖。這些位置權杖是用於指派及管理使用 Apple Business Manager 購買的授權。內容管理員可以在 Apple Business Manager 中購買並使用具備權限的位置權杖與授權建立關聯。接著會從 Apple Business Manager 下載這些位置權杖，並在 Microsoft Intune 中上傳它們。Microsoft Intune 支援針對每個租用戶上傳多個位置權杖。每個權杖有效期限為一年。

NOTE

Apple 大量採購方案 (VPP) 已整合到 Apple Business Manager。Apple Business Manager 是可供系統管理員部署 Apple 裝置並大量取得內容的入口網站。內容可能包括應用程式、書籍和自訂應用程式。位置權杖是用於指派及管理使用 Apple Business Manager 購買的授權。VPP 現在稱為舊版的 VPP 權杖。

已購買之應用程式的授權方式為何？

您可以使用 Apple 針對 iOS/iPadOS 和 macOS 裝置所提供的兩種授權類型，將已購買的應用程式指派給群組。

NOTE

裝置授權的 VPP 應用程式只能透過 MDM 通道安裝和更新。使用者無法直接前往市集以手動安裝或更新 VPP 應用程式。

II	IIII	IIIIII
App Store 登入	不需要。	在系統提示登入 App Store 時，每個使用者都必須使用唯一的 Apple ID。
裝置設定封鎖對 App Store 的存取	可以使用公司入口網站來安裝及更新應用程式。	您需要存取 App Store 才能加入 Apple Business Manager 的邀請。如果您已經設定原則來停用 App Store，則 VPP 應用程式的使用者授權將無法運作。

[[	[[[[	[[[[[[
自動應用程式更新	如 Intune 系統管理員在 Apple Business Manager 權杖設定中所設定的。 如果指派類型為 [適用於已註冊的裝置], 您也可以透過選取應用程式詳細資料頁面上的 [■] 動作, 從公司入口網站安裝可用的應用程式更新。	如 Intune 系統管理員在 Apple Business Manager 權杖設定中所設定的。 如果指派類型為 [適用於已註冊的裝置], 您也可以透過選取應用程式詳細資料頁面上的 [■] 動作, 從公司入口網站安裝可用的應用程式更新。
使用者註冊	不支援。	支援使用受控 Apple ID。
書籍	不支援。	支援。
已使用授權	每個裝置 1 個授權。授權會與裝置關聯。	1 個授權可用於使用相同個人 Apple ID 的 5 部裝置。授權會與使用者建立關聯。 在 Intune 中與個人 Apple ID 和受控 Apple ID 關聯的使用者會耗用 2 個應用程式授權。
授權移轉	只有在使用 [必要] 指派類型的情況下, 應用程式才能以無訊息方式從使用者授權移轉為裝置授權。	無論是哪種指派類型, 應用程式都無法從裝置授權移轉為使用者授權。

NOTE

公司入口網站不會在 [使用者註冊] 裝置上顯示裝置授權的應用程式, 因為在 [使用者註冊] 裝置上僅能安裝使用者授權的應用程式。

當您為 Apple 大量採購方案 (VPP) 建立新的指派時, 預設授權類型現在為「裝置」。現有的指派仍保持不變。

支援哪些應用程式類型？

您可以使用 Apple Business Manager 來購買並發佈公用及私人應用程式。

- **市集應用程式：**內容管理員可以使用 Apple Business Manager 取得 App Store 中所提供的免費和付費應用程式。
- **自訂應用程式：**內容管理員也可以使用 Apple Business Manager 取得以私人方式向貴組織提供的自訂應用程式。這些應用程式會由與您直接合作的開發人員, 針對您組織的特定需求量身打造。深入了解[如何散發自訂應用程式](#) (英文)。

必要條件

- 適用於您組織的 [Apple Business Manager](#) 或 [Apple School Manager](#) 帳戶。
- 已指派至一或多個位置權杖之已購買的應用程式授權。
- 已下載的位置權杖。

IMPORTANT

- 單一位置權杖同時只能搭配單一裝置管理解決方案使用。開始搭配 Intune 使用已購買的應用程式之前，請撤銷並移除搭配其他行動裝置管理 (MDM) 廠商使用的任何現有位置權杖。
- 單一位置權杖僅支援同時搭配單一 Intune 用戶端使用。請勿將相同的權杖重複用於多個 Intune 租用用戶。
- 根據預設，Intune 每天與 Apple 同步處理一次位置權杖。您可以隨時從 Intune 起始手動同步處理。
- 在您將位置權杖匯入到 Intune 之後，請不要將相同的權杖匯入到任何其他裝置管理解決方案。這樣做可能會導致授權指派與使用者記錄遺失。

從大量採購方案 (VPP) 移轉至「App 及書籍」

如果您的組織尚未移轉至 Apple Business Manager 或 Apple School Manager，請檢閱 [Apple 針對移轉至 \[App 及書籍\] 的指引](#)，再繼續於 Intune 中管理已購買的應用程式。

IMPORTANT

- 為了獲得最佳的移轉體驗，請針對每個位置僅移轉單一 VPP 購買者。如果每個購買者都移轉到唯一位置，所有的授權 (包括已指派和未指派的授權) 都會移轉至 [App 及書籍]。
- 請不要刪除 Intune 中的現有舊版 VPP 權杖，或是 Intune 中與現有舊版 VPP 權杖相關聯的應用程式和指派。這些動作將需要在 Intune 中重新建立所有應用程式指派。

在 Apple Business Manager 或 Apple School Manager 中將現有的已購買 VPP 內容和權杖移轉至 [App 及書籍] 的步驟如下：

1. 邀請 VPP 購買者加入您的組織，並引導每個使用者選取唯一的位置。
2. 在繼續之前，請確定組織內的所有 VPP 購買者都已完成步驟 1。
3. 確認所有已購買的應用程式和授權都已經移轉至 Apple Business Manager 或 Apple School Manager 中的 [App 及書籍]。
4. 透過移至 [Apple Business (或 School) Manager] > [設定] > [App 及書籍] > [我的伺服器權杖] 來下載新的位置權杖。
5. 透過移至 [租用戶系統管理] > [連接器與權杖] > [Apple VPP 權杖] 來更新 Microsoft 端點管理員系統管理中心中的位置權杖，並手動上傳權杖。

上傳 Apple VPP 或 Apple Business Manager 位置權杖

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [租用戶系統管理] > [連接器與權杖] > [Apple VPP 權杖]。
3. 在 VPP 權杖清單窗格上，選取 [建立]。[建立 VPP 權杖] 程序隨即顯示。建立 VPP 權杖時，會使用四個頁面。第一個是 [基本]。
4. 在 [基本] 頁面上，指定下列資訊：
 - **權杖名稱** - 用於設定權杖名稱的系統管理欄位。
 - **Apple ID** - 輸入與已上傳權杖相關聯的帳戶的受控 Apple ID。
 - **VPP 權杖檔案** - 如果您尚未這麼做，請註冊 Apple Business Manager 或 Apple School Manager。註冊之後，請在這裡下載並選取您帳戶的 Apple Business Manager 位置權杖 (Apple VPP 權杖)。
5. 按一下 [下一步] 以顯示 [設定] 頁面。
6. 在 [設定] 頁面上，指定下列資訊：
 - **從其他 MDM 中控制權杖** - 將此選項設定為 [是]，以允許從其他 MDM 解決方案將權杖重新指派給 Intune。
 - **國家/地區** - 選取 VPP 國家/地區市集。Intune 會從指定的 VPP 國家/地區市集同步所有地區設定的 VPP 應用程式市集。

WARNING

變更國家/地區將會針對搭配此權杖所建立的應用程式，在下次與 Apple 服務進行更新時更新應用程式中繼資料和 App Store URL。如果應用程式不存在於新的國家/地區市集，即不會更新應用程式。

- VPP 帳戶類型 - 請選擇 [商務] 或 [教育]。
- 自動更新應用程式 - 請選擇 [是] 或 [否] 以啟用自動更新。啟用時，Intune 會偵測 app store 內的 VPP 應用程式更新，並在裝置簽入時將更新自動推送至裝置。

NOTE

Apple VPP 應用程式的自動應用程式將會針對 ■ 與 ■ 安裝意圖自動更新。針對使用 ■ 安裝意圖部署的應用程式，自動更新會自動為 IT 系統管理員產生狀態訊息，通知已有可用的新版本應用程式。透過選取應用程式、選取 [裝置安裝狀態]，然後檢查 [狀態詳細資料]，即可看到此狀態訊息。

更新 VPP 應用程式時，裝置最多可能需要 24 小時才能接收更新的 VPP 應用程式。裝置必須解除鎖定，才能成功安裝更新。

- 我授權給 Microsoft 傳送使用者及裝置資訊到 Apple。 - 您必須選取 [我同意] 才能繼續。若要檢視 Microsoft 將哪些資料傳送給 Apple，請參閱 [Intune 傳送至 Apple 的資料](#)。

7. 按一下 [下一步] 以顯示 [範圍標籤] 頁面。
8. 按一下 [選取範圍標籤] 來選擇性地為應用程式新增範圍標籤。如需詳細資訊，請參閱 [針對分散式 IT 使用角色型存取控制 \(RBAC\) 和範圍標籤](#)。
9. 按一下 [下一步] 以顯示 [檢視 + 建立] 頁面。檢閱您針對 VPP 權杖所輸入的值與設定。
10. 完成時按一下 [建立]。該權杖會顯示在權杖清單窗格內。

同步 VPP 權杖

您可以在 Intune 中針對選取的權杖選擇 [同步]，來同步您已購買之應用程式的應用程式名稱、中繼資料和授權資訊。

指派大量採購應用程式

1. 選取 [應用程式] > [所有應用程式]。
2. 在應用程式清單窗格上，選擇您要指派的應用程式，然後選擇 [屬性]。選取位於 [指派] 旁的 [編輯]。
3. 在 [指派] 索引標籤上，選擇應用程式為 [必要的] 或 [適用於已註冊的裝置]。
4. 在您選取的指派類型底下，選擇 [新增群組]，然後在 [選取群組] 窗格上選擇您想要指派應用程式的 Azure AD 使用者或裝置群組。

NOTE

當您為 Apple 大量採購方案 (VPP) 建立新的工作分派時，預設授權類型為「裝置」。現有的指派仍保持不變。

5. 完成之後，請選擇 [儲存]。

NOTE

可用的部署用途不支援裝置群組，僅支援使用者群組。顯示的應用程式清單與權杖有關。如果您的應用程式與多個 VPP 權杖有相關聯，您會看到相同的應用程式顯示多次；每個權杖顯示一次。

NOTE

在使用者起始應用程式安裝之前，指派為 [可用] 的應用程式不會在裝置上受控。一旦已安裝指派為 [可用] 的應用程式，或使用者嘗試安裝應用程式，Intune 會確保應用程式已獲得授權。

NOTE

Intune (或任何其他 MDM) 實際上不會安裝 VPP 應用程式。相反地，Intune 會連線到您的 VPP 帳戶，並告訴 Apple 要將哪些應用程式授權指派給哪些裝置。從該位置，所有實際安裝都會在 Apple 與裝置之間處理。

VPP 的使用者提示

終端使用者將會在許多案例中收到 VPP 應用程式安裝的提示。下表說明每個條件：

#	「	[[[APPLE VPP]]	[[[[[[[[	[[[APPLE ID
1	BYOD – 授權的使用者 (非「使用者註冊裝置」裝置)	Y	Y	Y
2	公司 – 授權的使用者 (不受監督的裝置)	Y	Y	Y
3	公司 – 授權的使用者 (受監督的裝置)	Y	N	Y
4	BYOD – 授權的裝置	N	Y	N
5	公司 – 授權的裝置 (不受監督的裝置)	N	Y	N
6	公司 – 授權的裝置 (受監督的裝置)	N	N	N
7	Kiosk 模式 (受監督的裝置) – 授權的裝置	N	N	N
8	Kiosk 模式 (受監督的裝置) – 授權的使用者	---	---	---

NOTE

不建議將 VPP 應用程式指派給使用使用者授權的 Kiosk 模式裝置。

撤銷應用程式授權

您可以根據指定的裝置、使用者或應用程式，撤銷所有相關聯的 iOS/iPadOS 或 macOS 大量採購方案 (VPP) 應用程式授權。但 iOS/iPadOS 和 macOS 平台之間有一些差異。

「	IOS/IPADOS	MACOS

II	IOS/IPADOS	MACOS
移除應用程式指派	移除應用程式指派是撤銷應用程式授權的先決條件。當您移除使用者的應用程式指派時，在您將指派變更為 [■] 之前，Intune 不會回收使用者或裝置授權。如果在安裝應用程式時移除應用程式指派，而且從未指派為 [■]，它仍會保持安裝狀態，但將不再提供安裝給使用者或裝置。	移除應用程式指派是撤銷應用程式授權的先決條件。當您移除使用者的應用程式指派時，在您將指派變更為 [■] 之前，Intune 不會回收使用者或裝置授權。如果在安裝應用程式時移除應用程式指派，而且從未指派為 [■]，它仍會保持安裝狀態，但將不再提供安裝給使用者或裝置。
撤銷應用程式授權	將應用程式指派變更為 [■] 之後，您可以使用 [■] 動作，從使用者或裝置回收應用程式授權。您必須將指派變更為 [■]，才能從裝置移除應用程式，並撤銷應用程式授權。	將應用程式指派變更為 [■] 之後，您可以使用 [■] 動作，從使用者或裝置回收應用程式授權。具有已撤銷授權的 macOS 應用程式仍可在裝置上使用，但必須等到將授權重新指派給使用者或裝置之後，才能更新。根據 Apple，這類應用程式會在 30 天的寬限期後移除。您必須將指派變更為 [■]，才能從裝置移除應用程式，並撤銷應用程式授權。

NOTE

- 當員工離職且不再屬於 AAD 群組時，Intune 會回收應用程式授權。
- 將 [解除安裝] 意圖指派給已購買的應用程式時，Intune 會同時回收授權並解除安裝應用程式。
- 從 Intune 管理移除裝置時，並不會回收應用程式授權。
- 當使用者從 Azure AD 中刪除時，Intune 會撤銷應用程式授權。

刪除 VPP 權杖

您可以使用主控台來刪除 Apple 大量採購方案 (VPP) 權杖。當您擁有重複的 VPP 權杖執行個體時，這可能是必要的。刪除權杖也會刪除任何相關聯的應用程式和指派。刪除權杖會撤銷相關聯的應用程式授權，但不會將應用程式解除安裝。

NOTE

刪除權杖之後，Intune 無法撤銷應用程式授權。

若要撤銷指定 VPP 權杖的所有 VPP 應用程式的授權，您必須先撤銷與權杖相關聯的所有應用程式授權，然後刪除權杖。

更新 VPP 權杖或 Apple Business Manager 位置權杖

您可以藉由從 [Apple Business Manager](#) 或 [Apple School Manager](#) 再次下載權杖並更新 Intune 中的現有權杖，來更新 Apple Business Manager 位置權杖 (Apple VPP 權杖)。

若要更新 Apple Business Manager 位置權杖 (Apple VPP 權杖)，請使用下列步驟：

- 瀏覽至 [Apple Business Manager](#) 或 [Apple School Manager](#)。
- 在 Apple Business (或 School) Manager 中，選取 [喜好 > 設定 收費和計費 > 應用程式和書籍 > 伺服器權杖]，以下載現有的權杖。
- 選取 [租用戶系統管理] > [連接器與權杖] > [Apple VPP 權杖]，更新 [Microsoft 端點管理員系統管理中心](#) 的權杖。
- 選取您要更新的 VPP 權杖、按一下 [基本] 類別上的 [編輯]、在此頁面上傳新權杖，然後儲存您的變更。

NOTE

當使用者已在 Apple Business Manager 中設定權杖，變更了其密碼或離開您的 Apple Business Manager 組織時，您必須更新現有的 Apple VPP 權杖或位置權杖。未更新的權杖會在 Intune 中顯示「無效」狀態。

刪除 VPP 應用程式

您可以刪除未與應用程式相關聯的可用或已使用授權的已購買應用程式。這可能需要清除不再指派的應用程式。

若要刪除 VPP 應用程式，請使用下列步驟：

1. 在 [Apple Business manager](#) 或 [Apple School manager](#) 中建立新的位置。
2. 撤銷使用相關聯位置權杖之應用程式的所有授權。在 [Microsoft 端點管理員系統管理中心](#) 中，選取 **應用程式 > 所有應用程式 > 選取該應用程式以刪除 > 應用程式授權 > 撤銷授權**。
3. 在 Apple Business Manager 或 Apple School Manager 中，將應用程式的所有授權從原始位置傳輸至新位置。
4. 同步位於 [Microsoft 端點管理員系統管理中心](#) 的位置權杖。
5. 在 [Microsoft 端點管理員系統管理中心](#) 中刪除該應用程式，選取 **應用程式 > 所有應用程式 > 以滑鼠右鍵點一下要刪除的應用程式 > 刪除**。

刪除 VPP 應用程式會導致下列結果：

- 將移除相關聯的應用程式指派。
- 如果 VPP 應用程式在嘗試刪除時已指派授權，您將會看到錯誤。

NOTE

系統不會刪除與 VPP 權杖相關聯的已購買書籍。

指派 VPP 的自訂角色權限

您可以在 Intune 中使用指派給自訂系統管理員角色的權限，獨立控制對 Apple Business Manager 位置權杖和應用程式 (Apple VPP 權杖和 VPP 應用程式) 的存取。

- 若要允許 Intune 自訂角色管理 Apple Business Manager 位置權杖，請在 [Microsoft 端點管理員系統管理中心](#) 內，選取 [租用戶系統管理] > [連接器與權杖] > [Apple VPP 權杖]，指派 **受控應用程式** 的權限。
- 若要允許 Intune 自訂角色管理在 [應用程式] > [所有應用程式] 底下使用 iOS/iPadOS VPP 權杖購買的應用程式，請指派適用於 [行動應用程式] 的權限。

其他資訊

Apple 提供建立和更新 VPP 權杖的直接協助。如需詳細資訊，請參閱 Apple 文件中的 [使用大量採購計劃 \(VPP\) 發佈內容給使用者](#)。

如果在 Intune 中指出 **已指派給外部 MDM**，您 (系統管理員) 必須先從協力廠商 MDM 移除 VPP 權杖，才能在 Intune 中使用 VPP 權杖。

若權杖的狀態是 **重複**，即表示已上傳多個具有相同 **權杖位置** 的權杖。請移除重複的權杖，以再次開始同步權杖。您仍能為標記為「重複」的權杖指派及撤銷授權。然而，權杖標記為「重複」之後，可能無法反映新購買的應用程式和書籍授權。

常見問題集

我可以上傳幾個權杖？

您可以在 Intune 中上傳最多 3,000 個權杖。

在裝置上安裝或移除應用程式之後，入口網站需要多久的時間才能更新授權數量？

在安裝或解除安裝應用程式之後的幾小時內，應該就會更新授權。請注意，如果使用者從裝置移除應用程式，該授權仍然會指派給該使用者或裝置。

是否可以過度訂閱應用程式，如果可以，是在怎樣的情況下？

是。Intune 系統管理員可以過度訂閱應用程式。例如，如果系統管理員購買 100 份 XYZ 應用程式的授權，然後將該應用程式的對象設為一個有 500 個成員的群組。前 100 個成員 (使用者或裝置) 將會獲得授權指派，其餘成員的授權指派則會失敗。

NOTE

當已使用的授權數量大於或等於特定應用程式總可用授權的 50% 時，警示會出現在 [註冊警示] 索引標籤下。當已使用的授權數量小於應用程式可用授權總數的 50% 時，警示就會消失。

後續步驟

請參閱 [如何監視應用程式](#)，以取得協助您監視應用程式指派的資訊。

請參閱 [如何對應用程式進行疑難排解](#)，來取得對應用程式相關問題進行疑難排解的相關資訊。

如何使用 Microsoft Intune 從商務用 Microsoft Store管理大量採購的應用程式

2022/9/27 •

商務用 Microsoft Store提供您一個位置，讓您能夠個別或大量地尋找及購買貴組織的應用程式。藉由將市集連線至 Microsoft Intune，您可以從入口網站管理大量採購的應用程式。例如：

- 您可以使用 Intune 同步處理您已購買 (或從市集免費) 的應用程式清單。
- 同步處理的應用程式會出現在Intune管理主控台中;您可以像指派任何其他應用程式一樣指派這些應用程式。
- 線上和離線授權的應用程式版本都會同步至Intune。應用程式名稱會在入口網站中附加「線上」或「離線」。
- 您可以追蹤可用的授權數目，以及Intune管理主控台中使用的授權數目。
- 如果可用的授權數目不足，Intune封鎖應用程式的指派和安裝。
- Intune會在使用者從 Azure AD 中刪除時，撤銷商務用 Microsoft Store所管理應用程式的應用程式授權。

開始之前

IMPORTANT

商務用 Microsoft Store將於 2023 年第一季淘汰。不過，在 2023 年淘汰之前，系統管理員仍然可以利用連線從其 UEM 解決方案Microsoft Store商務與教育版，將應用程式部署到受控Windows 11裝置。

開始同步處理並從商務用 Microsoft Store指派應用程式之前，請先檢閱下列資訊：

- 將Intune設定為貴組織的行動裝置管理授權單位。
- 您必須在商務用 Microsoft Store上註冊帳戶。
- 一旦您將 Microsoft 商務Microsoft Store帳戶與Intune相關聯之後，就無法在未來變更為不同的帳戶。
- 從市集購買的應用程式無法從Intune手動新增或刪除。它們只能與商務用 Microsoft Store同步處理。
- 您從商務用 Microsoft Store購買的線上和離線授權應用程式都會同步至Intune。然後，您可以將這些應用程式部署到裝置群組或使用群組。
- 線上應用程式安裝是由市集管理。
- 免費的離線應用程式也可以同步至Intune。這些應用程式是由Intune安裝，而不是由市集安裝。
- 若要使用這項功能，裝置必須加入Active Directory 網域服務、加入 Azure AD 或加入工作場所。
- 已註冊的裝置必須使用 1511 版的 Windows 10 或更新版本。

NOTE

線上商務用 Microsoft Store應用程式只能用於使用者內容安裝;也就是說，透過Intune部署時，您需要以使用者群組為目標。裝置授權離線商務用 Microsoft Store應用程式可以安裝在裝置內容中;也就是說，透過Intune部署時，您可以將裝置群組和使用群組設為目標。

NOTE

如果您透過原則或群組原則) 手動停用受管理裝置上 (存取Microsoft Store，線上授權應用程式將無法安裝。

將您的商務用 Microsoft Store帳戶與Intune

在Intune主控台中啟用同步處理之前，您必須先將市集帳戶設定為使用Intune作為管理工具：

1. 請確定您使用您用來登入Intune的相同租使用者帳戶來登入商務用 Microsoft Store。
2. 在商務Microsoft Store中，選擇 [管理] 索引標籤，選取 [設定]，然後選擇 [散發] 索引卷標。
3. 如果您沒有以 行動 裝置管理工具Microsoft Intune，請選擇 [新增管理工具] 以新增 Microsoft Intune。如果您沒有 Microsoft Intune 啟用為行動裝置管理工具，請按一下 [Microsoft Intune] 旁的 [啟用]。請注意，您應該啟用Microsoft Intune，而不是 Microsoft Intune註冊。

NOTE

您先前只能建立一個管理工具的關聯，以指派應用程式與商務用 Microsoft Store。您現在可以將多個管理工具與存放區建立關聯，例如，Intune和Configuration Manager。

您現在可以在 Intune 主控台中繼續並設定同步處理。

設定同步處理

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [租使用者系統管理 > 連接器和權杖 > 商務用 Microsoft Store]。
3. 按一下 [啟用]。
4. 如果您尚未這麼做，請按一下連結以註冊商務用 Microsoft Store，並如先前所述將您的帳戶建立關聯。
5. 從 [語言] 下拉式清單中，選擇入口網站中顯示商務用 Microsoft Store應用程式的語言。不論顯示的語言為何，它們都會在可用時以使用者的語言安裝。
6. 按一下 [同步]，將您從Microsoft Store購買的應用程式放入Intune。

同步處理應用程式

如果您已經將商務用 Microsoft Store帳戶與Intune系統管理員認證建立關聯，您可以使用下列步驟手動同步處理商務用 Microsoft Store應用程式與Intune。

1. 選取 [租使用者系統管理 > 連接器和權杖 > 商務用 Microsoft Store]。
2. 按一下 [同步]，將您從Microsoft Store購買的應用程式放入Intune。

NOTE

目前不支援具有加密應用程式套件的應用程式，且不會同步至Intune。

指派應用程式

您從市集指派應用程式的方式，與指派任何其他Intune應用程式的方式相同。如需詳細資訊，請參閱[如何將應用程式指派給具有Microsoft Intune的群組](#)。

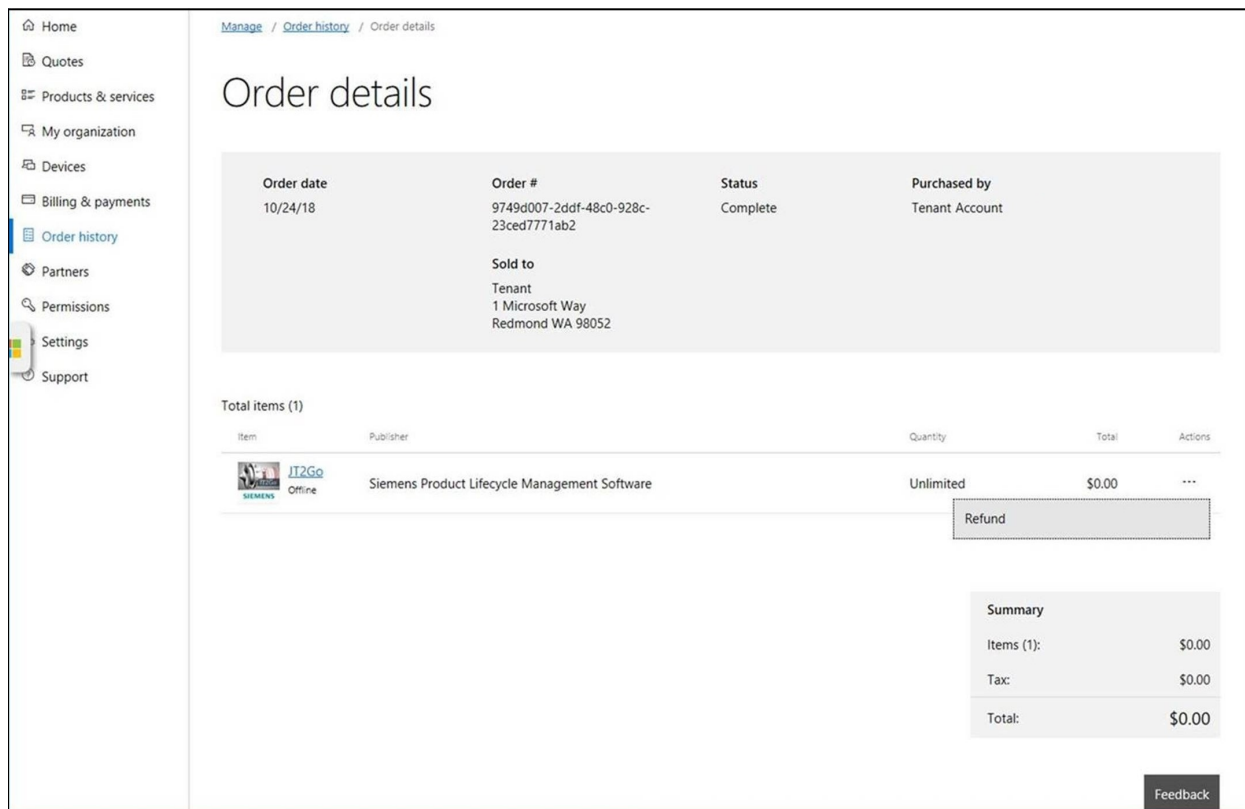
離線應用程式可以以使用者群組、裝置群組或具有使用者和裝置的群組為目標。離線應用程式可以針對裝置上的特定使用者或裝置上的所有使用者安裝。

當您指派商務用 Microsoft Store應用程式時，安裝應用程式的每個使用者都會使用授權。如果您針對指派的應用程式使用所有可用的授權，就無法再指派任何複本。採取下列其中一個動作：

- 從某些裝置卸載應用程式。
- 減少目前指派的範圍，僅以您擁有足夠授權的使用者為目標。
- 從商務用 Microsoft Store購買更多應用程式複本。

移除應用程式

若要移除從商務用 Microsoft Store 同步處理的應用程式，您必須登入商務用 Microsoft Store 並退款應用程式。無論應用程式是否免費，程式都相同。針對免費應用程式，市集會退款 \$0。下列範例顯示免費應用程式的退款。



The screenshot shows the 'Order details' page in the Microsoft Store. The left sidebar contains navigation links: Home, Quotes, Products & services, My organization, Devices, Billing & payments, Order history (selected), Partners, Permissions, Settings, and Support. The main content area displays order information:

Order date	Order #	Status	Purchased by
10/24/18	9749d007-2ddf-48c0-928c-23ced7771ab2	Complete	Tenant Account

Sold to:
Tenant
1 Microsoft Way
Redmond WA 98052

Total items (1)

Item	Publisher	Quantity	Total	Actions
 IT2Go Offline	Siemens Product Lifecycle Management Software	Unlimited	\$0.00	...

A 'Refund' button is visible next to the item.

Summary

Items (1):	\$0.00
Tax:	\$0.00
Total:	\$0.00

A 'Feedback' button is located at the bottom right.

NOTE

移除應用程式在私人市集中的可見度並不會讓Intune同步處理應用程式。您必須將應用程式退款，才能完全移除應用程式。

後續步驟

- 使用 [Microsoft Intune](#) 管理大量採購的應用程式和書籍

如何使用 Microsoft Intune 管理透過大量購買程式所購買的 iOS/iPadOS eBooks

2022/9/27 •

Apple Volume Purchase Program (VPP) 可讓您購買要散佈至公司使用者之書的多個授權。您可以從商務或教育存放區中分配圖書。

Microsoft Intune 會協助您同步處理、管理與指派您透過此程式購買的圖書。您可以從儲存區匯入授權資訊，並追蹤您使用的授權數目。

管理圖書的程式類似于 [管理 VPP 應用程式](#)。

管理 iOS 裝置的大量購買的圖書

您可以透過 [Apple Business manager](#) 或 [apple School manager](#) 取得 iOS/iPadOS 帳簿的多個授權。此套裝程式含從 Apple 網站設定 Apple Business Manager 帳戶，以及將位置權杖上傳至 Intune 的過程。然後，您可以使用 Intune 同步處理大量購買資訊，並追蹤大量購買的圖書使用。

開始之前

開始之前，請從 Apple 取得 VPP 權杖，並將其上傳至您的 Intune 帳戶。此外：

- 如果您先前使用的 VPP 權杖與不同的產品，您必須產生新的憑證以與 Intune 搭配使用。
- 每個權杖的有效年份為一年。
- 依預設，Intune 會一天兩次同步處理 Apple Business Manager 服務。您可以隨時啟動手動同步處理。
- 將 VPP 權杖匯入至 Intune 後，請勿將相同的權杖匯入任何其他裝置管理解決方案。這樣做可能會導致授權指派和使用者記錄遺失。
- 在您開始使用具有 Intune 的 iOS/iPadOS 帳簿之前，請先移除其他行動裝置管理 (MDM) 廠商所建立的任何現有 VPP 使用者帳戶。Intune 不會將這些使用者帳戶同步處理成 Intune 的安全性度量。Intune 只會同步處理來自 Intune 所建立之 Apple Business Manager 服務的資料。
- 當您指派書給裝置時，該裝置必須已安裝內建的 iBooks 應用程式。如果不是，則使用者必須先重新安裝應用程式，才能閱讀該書。您目前無法使用 Intune 還原已移除的內建應用程式。
- 您只能從 Apple Volume Purchase Program 網站指派圖書。您無法上傳，然後指派您內部建立的書。
- 您目前無法將書籍指派給使用者類別，與執行應用程式的方式相同。
- 一旦指派書，您就無法收回授權。
- 當具有合格裝置的使用者第一次嘗試安裝 VPP 圖書時，必須先加入 Apple Volume Purchase program，才能安裝該書。您也可以使用 managed Apple IDs，將授權指派給安全性群組。如果您這麼做，則在安裝手冊時，不會提示使用者輸入其 Apple ID。
- 裝置必須使用使用者親近性註冊，因為電子書只可指派給使用者群組。

取得及上傳 Apple Business Manager 位置 token

1. 登入 Microsoft 端點管理員系統 [管理中心](#)。
2. 選取 **租使用者管理** > **連接器和權杖** > **Apple VPP 權杖**。
3. 在 [VPP 權杖] 窗格的清單中，按一下 [建立]。
4. 在 [新增 VPP 權杖] 窗格上，指定下列資訊：
 - **VPP 權杖 檔案**-確保您已登入 [apple Business Manager](#) 或 [apple School manager](#)。請注意，這些服務先前稱為「Apple 的商務用的 Apple 大量購買程式」或「Apple 大量購買計畫教育版」。然後，下載您帳戶

的 Apple 位置/VPP 權杖，並在端點管理員中加以選取。

- **APPLE id** -輸入與 volume purchase program 相關聯之帳戶的 Apple ID。
- **VPP 帳戶類型** -從 **商務** 或 **教育** 版選擇。

5. 完成後，按一下 [**建立**]。

權杖會顯示在 [標記] 窗格的清單中。

您可以隨時選擇 [**同步 處理**]，以隨時同步處理 Apple 與 Intune 所保留的資料。

指派大量購買的應用程式

1. 選取 [**app > eBooks > All eBooks**]。
2. 在 [圖書] 窗格的清單中，選擇您要指派的圖書，然後選擇 [> **指派群組** **]。 **
3. 在 [< **手冊名稱** > **指派的群組**] 窗格中，選擇 [**管理 > 群組指派**]。
4. 選擇 [**指派群組**]，然後在 [**選取群組**] 窗格中，選擇您要指派書的 Azure AD 使用者群組。目前不支援裝置群組。選擇 [**可用** 的指派動作] 或 [**必要**]。
5. 完成後，請選擇 [**儲存**]。

後續步驟

請參閱 [如何監視應用程式](#) 以取得資訊，以協助您監視圖書工作。

如何只抹除 Intune 管理之應用程式中的公司資料

2022/9/27 •

當裝置遺失或遭竊，或員工離職時，您想要確定公司應用程式資料已從裝置中移除。但您可能不想移除裝置上的個人資料，特別是當裝置是員工擁有的裝置時。

NOTE

iOS/iPadOS、Android 和 Windows 10 平臺是目前唯一支援從受控應用程式抹除公司資料Intune平臺。Intune受控應用程式是包含Intune APP SDK 的應用程式，而且在您的組織中至少有一個啟用和授權的使用者帳戶。需要部署應用程式保護原則，才能在 Android 和 iOS 上啟用應用程式選擇性抹除。

若要選擇性地移除公司應用程式資料，請使用本主題中的步驟來建立抹除要求。要求完成之後，下次應用程式在裝置上執行時，會從應用程式中移除公司資料。此外，您也可以在不符合應用程式保護原則 (應用程式) 存取設定的條件時，將公司資料的選擇性抹除設定為新的動作。這項功能可協助您根據預先設定的準則，自動保護及移除應用程式中的敏感性公司資料。

IMPORTANT

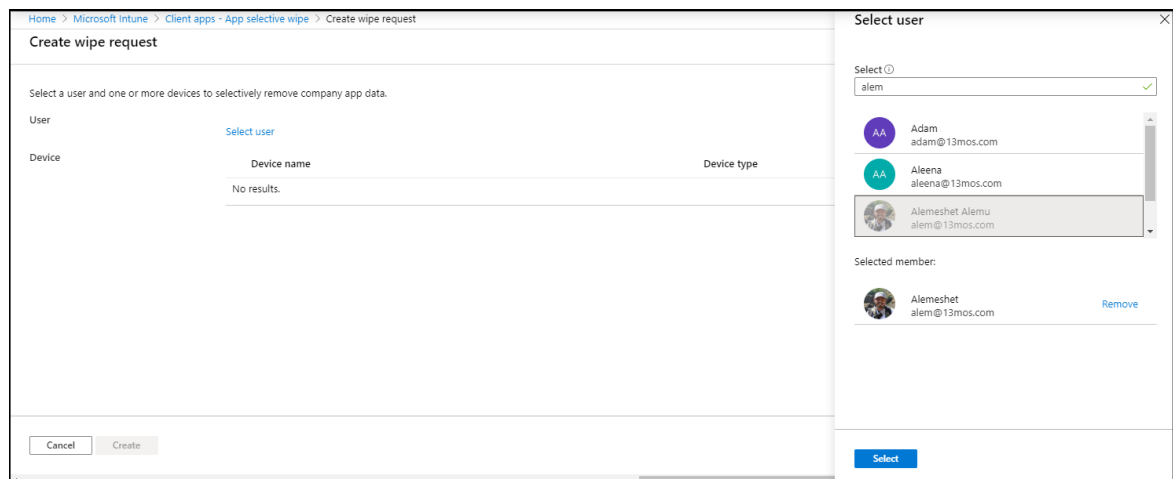
系統會移除直接從應用程式同步至原生通訊錄的連絡人。無法抹除從原生通訊錄同步到另一個外部來源的任何連絡人。目前，這僅適用於 Microsoft Outlook 應用程式。

已部署不含使用者註冊的 WIP 原則

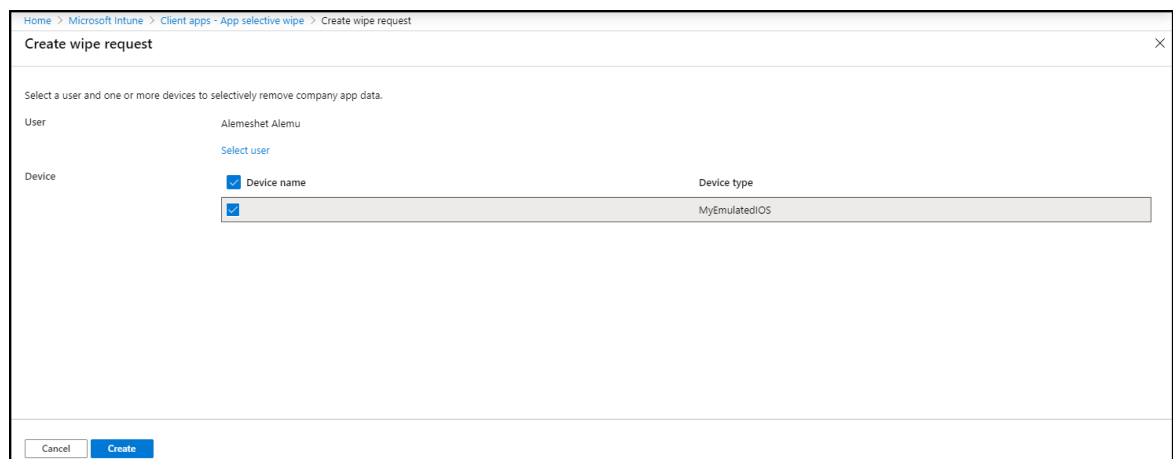
Windows 資訊保護 (WIP) 原則可以部署，而不需要 MDM 使用者註冊其Windows 10裝置。此設定可讓公司根據 WIP 設定來保護其公司檔，同時允許使用者維護自己Windows裝置的管理。使用 WIP 原則保護檔之後，Intune系統管理員 (全域管理員或[Intune服務系統管理員](#)) 可以選擇性地抹除受保護的資料。藉由選取使用者和裝置，並傳送抹除要求，所有透過 WIP 原則保護的資料都會變成無法使用。從入口網站的Intune中，選取 [\[用戶端應用程式\] > \[應用程式選擇性抹除\]](#)。如需詳細資訊，請參閱 [使用 Intune 建立和部署 Windows 資訊保護 \(WIP\) 應用程式保護原則](#)。

建立裝置型抹除要求

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [\[應用程式\] > \[應用程式選擇性抹除\] > \[建立抹除要求\]](#)。
[\[建立抹除要求\]](#) 窗格隨即顯示。
3. 按一下 [\[選取使用者\]](#)，選擇您要抹除其應用程式資料的使用者，然後按一下 [\[選取使用者\]](#) 窗格底部的 [\[選取\]](#)。

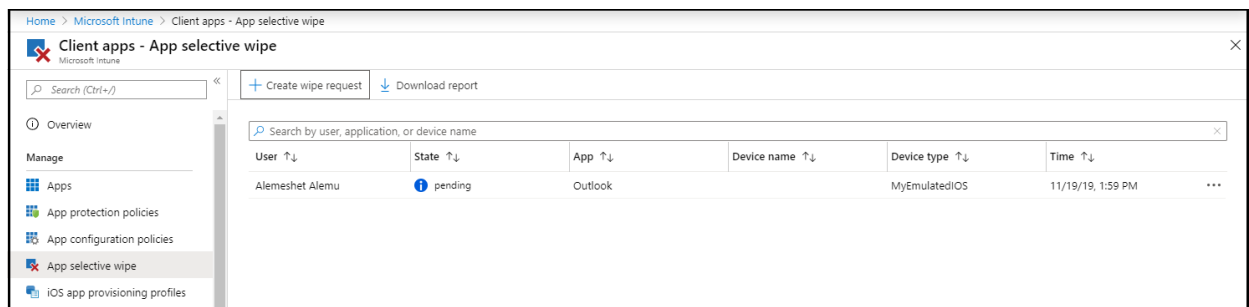


4. 按一下 [選取裝置]，選擇裝置，然後按一下 [選取裝置] 窗格底部的 [選取]。



5. 按一下 [建立] 提出抹除要求。

服務會針對裝置上每個受保護的應用程式，以及與抹除要求相關聯的使用者，建立並追蹤個別的抹除要求。



建立以使用者為基礎的抹除要求

藉由將使用者新增至使用者層級抹除，我們會自動對所有使用者裝置上的所有應用程式發出抹除命令。使用者會在每次從所有裝置簽入時繼續取得抹除命令。若要重新啟用使用者，您必須從清單中移除使用者。

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 >][應用程式選擇性抹除 >][使用者層級抹除]
3. 按一下 [新增] 並顯示 [選取使用者] 窗格。
4. 選擇您想要抹除其應用程式資料的使用者，然後按一下 [選取]。

監視抹除要求

您可以擁有摘要報告，其中顯示抹除要求的整體狀態，並包含擱置中要求和失敗的數目。完成的抹除要求專案會在完成後保留在報表中 4 天。如果抹除要求未標示為已完成，但仍處於暫止狀態，則要求會保留在報表中，總天

數等於離線寬限期抹除資料的值總和 + 要刪除記錄的 4 天，預設為 94 天。

若要取得更多詳細資料，請遵循下列步驟：

1. 在 [應用程式**][應用程式** > 選擇性抹除] 窗格中，您可以看到依使用者分組的要求清單。因為系統會為裝置上執行的每個受保護應用程式建立抹除要求，所以您可能會看到使用者的多個要求。狀態會指出抹除要求是 **擱置** 中、**失敗** 或 **成功**。

Wipe requests					
+ New wipe request					
USER	STATUS	APP	DEVICE NAME	DEVICE TYPE	TIME
▼ ...					
	Pending	Managed Browser		Nexus 9	11/07/16 1:38 PM ...
	Pending	OneDrive		iPad	11/07/16 1:38 PM ...
	Pending			iPad	2/06/17 10:49 PM ...
	Pending	PowerPoint		iPad	11/07/16 1:38 PM ...
	Pending	OneDrive		iPad	2/06/17 10:49 PM ...
	Pending	Word		iPad	11/07/16 1:38 PM ...
	Pending	OneDrive	Joseph's iPad	iPad	11/07/16 1:38 PM ...

此外，您也可以看到裝置名稱及其裝置類型，這在閱讀報表時很有說明。

IMPORTANT

使用者必須開啟應用程式，才能進行抹除，而且在提出要求後最多可能需要 30 分鐘的時間。

刪除裝置抹除要求

系統會顯示暫止狀態的抹除，直到您手動刪除它們為止。若要手動刪除抹除要求：

1. 在 [用戶端應用程式 - 應用程式選擇性抹除] 窗格上。
2. 從清單中，以滑鼠右鍵按一下您要刪除的抹除要求，然後選擇 [刪除抹除要求]。

Pending	Excel	...	2/06/17 10:49 PM	...
Pending	Outl	...	11/07/16 1:38 PM	...

Delete wipe request

3. 系統會提示您確認刪除，選擇 [是] 或 [否]，然後按一下 [確定]。

刪除使用者抹除要求

使用者抹除會保留在清單中，直到系統管理員移除為止。若要從清單中移除使用者：

1. 在 [用戶端應用程式 - 應用程式選擇性抹除] 窗格上，選取 [使用者層級抹除]
2. 從清單中，以滑鼠右鍵按一下您要刪除的使用者，然後選擇 [刪除]。

另請參閱

[什麼是應用程式保護原則](#)

應用程式防護原則概觀

2022/9/27 •

應用程式防護應用程式) (原則是確保組織資料保持安全或包含在受控應用程式中的規則。原則可以是使用者嘗試存取或移動「公司」資料時所強制執行的規則，或當使用者位於應用程式內時所禁止或監視的一組動作。受管理應用程式是已套用應用程式防護原則的應用程式，且可由 Intune 管理。

行動應用程式管理 (MAM) 應用程式保護原則可讓您管理和保護應用程式內的組織資料。許多生產力應用程式 (例如 Microsoft Office 應用程式) 都可由 Intune MAM 管理。請參閱可公開使用的 [Microsoft Intune 受保護應用程式](#) 官方清單。

如何保護應用程式資料

您的員工會使用行動裝置來處理個人和工作事務。在確保員工生產力的同時，您也會想要防止故意與無意的資料遺失。您也會想要為從不受您管理的裝置存取的公司資料提供保護。

您可以使用 Intune 與 **任何行動裝置管理 (MDM) 解決方案無關的** 應用程式保護原則。無論是否在裝置備管理解決方案中註冊裝置，這種獨立性可以幫助您保護公司的資料。藉由實作 **應用層級原則**，您可以限制對公司資源的存取，並將資料保留在 IT 部門的檢視範圍內。

裝置上的應用程式防護原則

您可以針對在下列裝置上執行的應用程式設定應用程式防護原則：

- 在 Microsoft Intune 中註冊：這些裝置通常是公司擁有的裝置。
- 已在協力廠商行動裝置管理 (MDM) 解決方案中註冊：這些裝置通常是公司擁有的。

NOTE

行動應用程式管理原則不應與協力廠商行動應用程式管理或安全容器解決方案搭配使用。

- 未在任何行動裝置管理解決方案中註冊：這些裝置通常是員工擁有的裝置，未在 Intune 或其他 MDM 解決方案中管理或註冊。

IMPORTANT

您可以為連線到 Microsoft 365 服務的 Office 行動裝置應用程式建立行動裝置應用程式管理原則。您也可以為啟用混合式新式驗證的 iOS/iPadOS 和 Android 版 Outlook 建立 Intune 應用程式防護原則，以保護 Exchange 內部部署信箱的存取權。使用此功能之前，請確定您符合 [iOS/iPadOS 和 Android 版 Outlook 的需求](#)。連線到內部部署 Exchange 或 SharePoint 服務的其他應用程式不支援應用程式防護原則。

使用應用程式防護原則的優點

使用應用程式防護原則的重要優點如下：

- 以應用程式層級保護您的公司資料。因為行動裝置應用程式管理不需要裝置管理，所以您可以保護受管理和未受管理裝置上的公司資料。此管理會以使用者身分識別為中心，這會對移除裝置管理的需求。
- 在個人環境中使用應用程式時，使用者生產力不會受到影響，而且不會套用原則。這些原則只會套用在工作內容中，讓您能夠保護公司資料，而不需要觸碰個人資料。
- 應用程式防護原則可確保實施應用程式層保護。例如，您可以：

- 需要 PIN 碼才能在工作內容中開啟應用程式
- 控制應用程式之間的資料共用
- 防止將公司應用程式資料儲存到個人儲存位置
- **除了 MAM 之外，MDM 也可確保裝置受到保護。**您可以要求 PIN 碼以存取裝置，或是將受管理應用程式部署到裝置。您也可以透過 MDM 解決方案將應用程式部署到裝置，讓您更充分掌控應用程式管理。

搭配使用 MDM 與應用程式防護原則還有其他優點，而且公司可以同時使用具有和不含 MDM 的應用程式防護原則。例如，假設有員工同時使用公司所簽發的電話，以及自己的個人平板電腦。公司電話已在 MDM 中註冊，並受到應用程式防護原則保護，而個人裝置僅受到應用程式防護原則的保護。

如果您在未設定裝置狀態的情況下將 MAM 原則套用至使用者，則使用者會在 BYOD 裝置和受 Intune 管理的裝置上取得 MAM 原則。您也可以根據受管理狀態套用 MAM 原則。因此，當您建立應用程式保護原則時，在 [所有應用程式類型的目標] 旁，您會選取 [否]。然後執行下列任何一項：

- 將較不嚴格的 MAM 原則套用至 Intune 受管理的裝置，並將更嚴格的 MAM 原則套用至未註冊 MDM 的裝置。
- 僅將 MAM 原則套用至未註冊的裝置。

應用程式防護原則支援的平臺

Intune 提供一系列功能，可協助您在您想要的裝置上，取得所需的應用程式。如需詳細資訊，請參閱 [依平臺的應用程式管理功能](#)。

Intune 應用程式保護原則平臺支援與 Android 和 iOS/iPadOS 裝置 Office 行動應用程式平臺支援一致。如需詳細資訊，請參閱 [Office 系統需求的行動應用程式](#) 一節。

IMPORTANT

裝置上需要 Intune 公司入口網站，才能在 Android 上接收應用程式防護原則。

應用程式防護原則資料保護架構

應用程式保護原則中可用的選項 (APP) 可讓組織根據其特定需求量身打造保護。對某些人而言，實作完整案例所需的原則設定可能不明顯。為了協助組織排定行動用戶端端點強化的優先順序，Microsoft 已針對其應用程式資料保護架構引進分類法，以進行 iOS 和 Android 行動應用程式管理。

APP 資料保護架構會組織成三個不同的組態層級，每個層級會根據上一個層級來建置：

- **Enterprise 層級 1 (基本資料保護)** 確保應用程式受到 PIN 保護並加密，並執行選擇性抹除作業。針對 Android 裝置，此層級會驗證 Android 裝置證明。這是一種進入層級設定，可在信箱原則 Exchange Online 提供類似的資料保護控制，並將 IT 和使用者母體引進 APP。
- **Enterprise 層級 2 (增強的資料保護)** 引進 APP 資料外泄防護機制和最低作業系統需求。這是適用於大部分存取公司或學校資料之行動使用者的設定。
- **Enterprise 高資料保護 (層級 3)** 引進進階資料保護機制、增強的 PIN 設定，以及 APP Mobile Threat Defense。此設定適用於存取高風險資料的使用者。

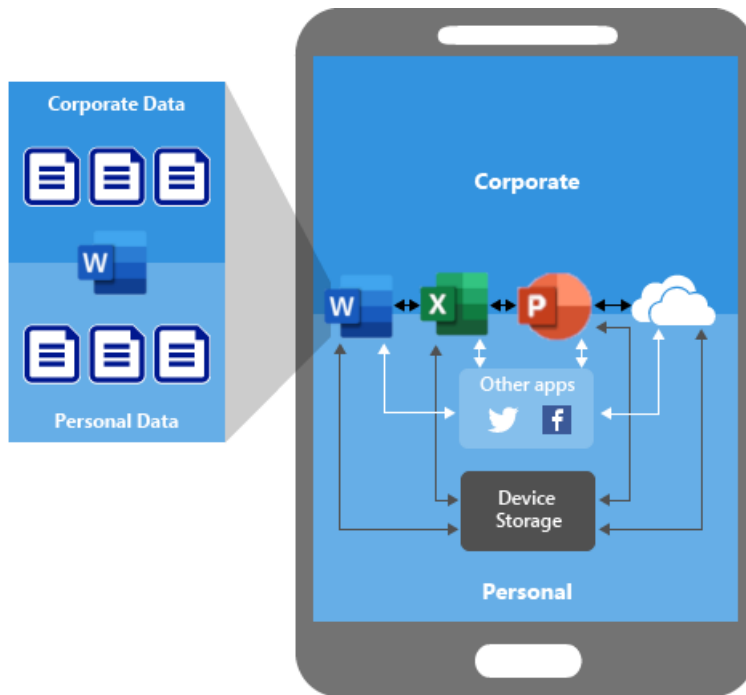
若要查看每個設定層級的特定建議，以及必須保護的最低應用程式，請 [檢閱使用應用程式保護原則的資料保護架構](#)。

應用程式保護原則如何保護應用程式資料

沒有應用程式防護原則的應用程式

使用沒有限制的應用程式時，公司和個人資料可能會交集在一起。公司資料最終可能會位於個人儲存體等位置，或傳輸至您 Purview 以外的應用程式，並導致資料遺失。下圖中的箭號顯示公司和個人應用程式之間，以及儲存

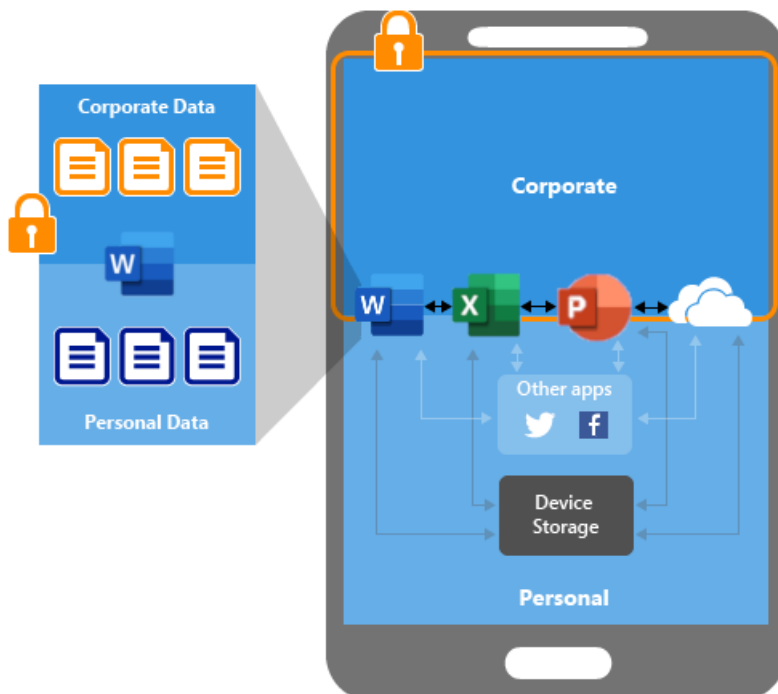
體位置之間的不受限制資料移動。



應用程式) (使用應用程式保護原則進行資料保護

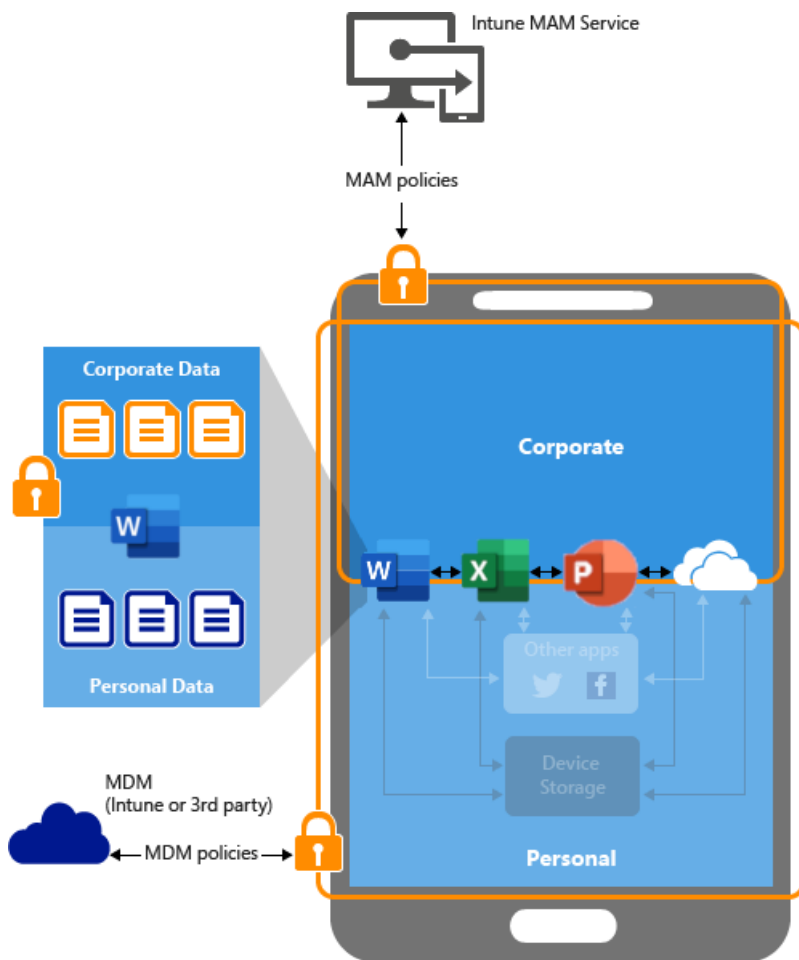
您可以使用應用程式防護原則來防止公司資料儲存到裝置的本機儲存體 (請參閱下圖)。您也可以將資料移動限制為不受應用程式防護原則保護的其他應用程式。應用程式防護原則設定包括：

- 資料重新配置原則，例如 儲存組織資料的複本，以及 限制剪下、複製和貼上。
- 存取原則設定，例如 需要簡單的 PIN 以進行存取，以及 封鎖受控應用程式在已越獄或 Root 破解的裝置上執行。



在 MDM 解決方案所管理的裝置上使用 APP 進行資料保護

下圖顯示 MDM 和應用程式防護原則一起提供的保護層級。



MDM 解決方案藉由提供下列專案來增加價值：

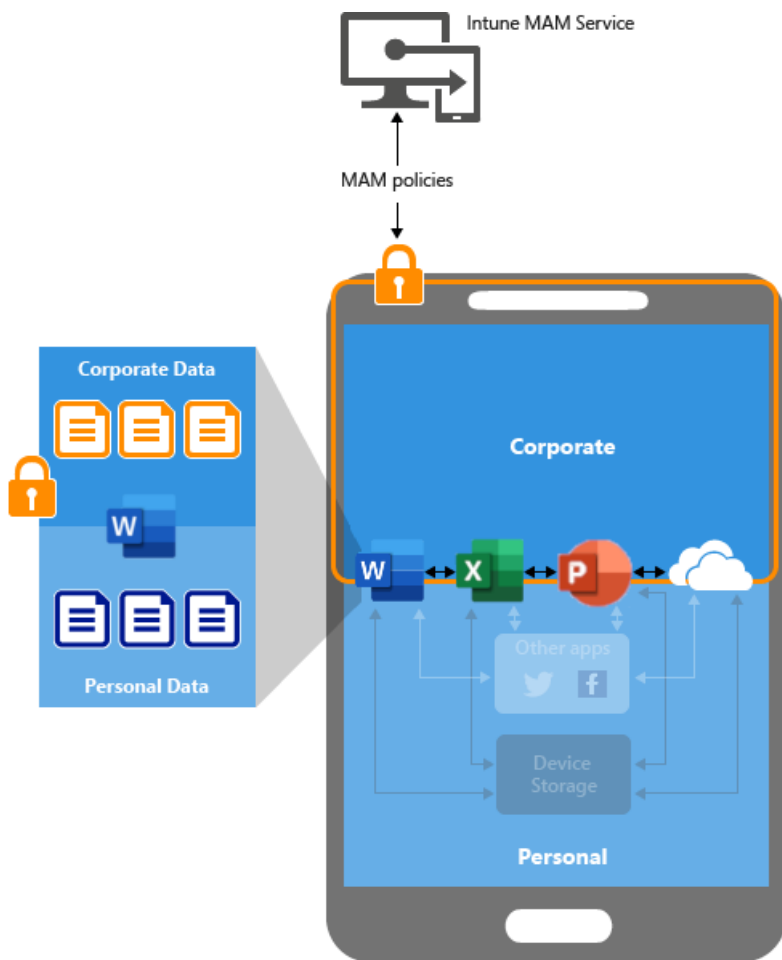
- 註冊裝置
- 將應用程式部署至裝置
- 提供持續的裝置合規性與管理

應用程式防護原則會藉由提供下列專案來增加價值：

- 協助保護公司資料免于洩漏至取用者應用程式和服務
- 將另 存新檔、剪貼簿 或 PIN 等限制套用至用戶端應用程式
- 視需要從應用程式抹除公司資料，而不從裝置移除這些應用程式

在不註冊的裝置上使用 APP 保護資料

下圖說明資料防護原則在沒有 MDM 的情況下，如何在應用層級運作。



對於未在任何 MDM 解決方案中註冊的 BYOD 裝置，應用程式防護原則可協助保護應用層級的公司資料。但是，要注意有某些限制，像是：

- 您無法將應用程式部署到裝置。終端使用者必須從市集取得應用程式。
- 您無法在這些裝置上佈建憑證設定檔。
- 您無法在這些裝置上佈建公司 Wi-Fi 和 VPN 設定。

您可以使用應用程式保護原則管理的應用程式

任何已與 [Intune SDK](#) 整合或由 Intune App Wrapping Tool 包裝的應用程式，都可以使用 [Intune](#) 應用程式保護原則來管理。請參閱已使用這些工具建置並可供公開使用的 [受保護 Microsoft Intune 應用程式](#) 官方清單。

Intune SDK 開發小組會主動測試並維護使用原生 Android、iOS/iPadOS (Obj-C、Swift)、Xamarin 和 Xamarin.Forms 平臺建置的應用程式支援。雖然有些客戶已成功 Intune SDK 與其他平臺整合，例如 React Native 和 NativeScript，但我們並未提供明確的指引或外掛程式，讓應用程式開發人員使用支援的平臺以外的任何專案。

使用應用程式保護原則的使用者需求

下列清單提供在受 Intune 管理的應用程式上使用應用程式保護原則的使用者需求：

- 使用者必須擁有 Azure Active Directory (Azure AD) 帳戶。請參閱 [新增使用者並授與系統管理許可權給 Intune](#)，以瞭解如何在 Azure Active Directory 中建立 Intune 使用者。
- 使用者必須具備指派給其 Azure Active Directory 帳戶的 Microsoft Intune 的授權。請參閱 [管理 Intune 授權](#)，以瞭解如何將 Intune 授權指派給使用者。
- 使用者必須屬於應用程式保護原則的目標安全性群組。相同的應用程式保護原則必須針對所使用的特定應用程式。應用程式防護原則可以在 Microsoft 端點管理員 [系統管理中心](#) 建立和部署。安全性群組目前可在 [Microsoft 365 系統管理中心](#) 中建立。

- 使用者必須使用 Azure AD 帳戶登入應用程式。

Microsoft Office應用程式的應用程式防護原則

搭配Microsoft Office應用程式使用應用程式防護原則時，有一些您需要注意的其他需求。

Outlook行動裝置應用程式

使用[Outlook行動裝置應用程式](#)的其他需求包括：

- 終端使用者必須將Outlook行動裝置應用程式安裝到其裝置上。
- 終端使用者必須有[連結至其Azure Active Directory帳戶的Microsoft 365 Exchange Online](#)信箱和授權。

NOTE

Outlook行動裝置應用程式目前僅支援Intune應用程式保護，以搭配[混合式新式驗證](#)Microsoft Exchange Online和Exchange Server，且不支援 Office 365 Dedicated 中的Exchange。

Word、Excel 和 PowerPoint

使用[Word、Excel 和 PowerPoint](#)應用程式的其他需求包括：

- 使用者必須擁有連結至其Azure Active Directory帳戶之[Microsoft 365 Apps 商務版或企業的授權](#)。訂用帳戶必須包含行動裝置上的Office應用程式，而且可以包含具有[商務用 OneDrive](#)的雲端儲存體帳戶。Microsoft 365可依照這些[指示](#)在[Microsoft 365 系統管理中心](#)中指派授權。
- 終端使用者必須在 [儲存組織資料的複本] 應用程式保護原則設定下，使用細微的儲存功能來設定受控位置。例如，如果受控位置OneDrive，則應在使用者的 Word、[Excel](#) 或 [PowerPoint](#)應用程式中設定OneDrive應用程式。
- 如果受控位置OneDrive，則應用程式必須以部署至使用者的應用程式保護原則為目標。

NOTE

Office行動裝置應用程式目前僅支援 SharePoint Online，而非內部部署SharePoint。

Office所需的管理位置

受控位置 (也就是Office需要OneDrive)。Intune將應用程式中的所有資料標示為「公司」或「個人」。資料來源自商務位置時會被視為「公司」。針對Office應用程式，Intune將下列專案視為商務位置：具有商務用 OneDrive帳戶的電子郵件 (Exchange) 或雲端儲存體 (OneDrive應用程式)。

商務用 Skype

使用 商務用 Skype還有其他需求。請參閱[商務用 Skype](#)授權需求。如需商務用 Skype (SfB) 混合式和內部部署設定，請參閱[混合式新式 SfB 驗證](#)和[Exchange](#)會分別使用[Azure AD 進行適用於 SfB OnPrem](#)的 GA 和新式驗證。

應用程式防護全域原則

如果OneDrive系統管理員流覽至 [admin.onedrive.com]，並選取 [裝置存取]，他們可以將行動應用程式 管理控制項設定為OneDrive和SharePoint用戶端應用程式。

這些設定可供OneDrive 管理員主控台使用，可設定稱為全域原則的特殊Intune應用程式 保護原則。此全域原則適用於您租使用者中的所有使用者，而且無法控制原則目標。

啟用之後，iOS/iPadOS 和 Android 的OneDrive和SharePoint應用程式預設會使用選取的設定來保護。IT Pro可以在 Intune 主控台中編輯此原則，以新增更具目標的應用程式，以及修改任何原則設定。

根據預設，每個租使用者只能有一個 全 局原則。不過，您可以使用[Intune Graph API](#)為每個租使用者建立額外的

全域原則，但不建議這麼做。不建議建立額外的全域原則，因為針對這類原則的實作進行疑難排解可能會變得複雜。

雖然 **全域** 原則會套用至租使用者中的所有使用者，但任何標準Intune應用程式保護原則都會覆寫這些設定。

NOTE

OneDrive 管理員中心內的原則設定已不再更新。您可以改用 Microsoft Endpoint Manager。如需詳細資訊，請參閱[控制OneDrive和SharePoint行動裝置應用程式中功能的存取權](#)。

應用程式防護功能

多重身分識別

多重身分識別支援可讓應用程式支援多個物件。這些物件同時是「公司」使用者和「個人」使用者。公司和學校帳戶是由「公司」物件使用，而個人帳戶則會用於取用者物件，例如Microsoft Office使用者。支援多重身分識別的應用程式可以公開發行，其中應用程式保護原則僅適用於在公司與學校（「公司」）內容中使用應用程式。多重身分識別支援會使用[Intune SDK](#)，只將應用程式保護原則套用到已登入應用程式的公司或學校帳戶。如果個人帳戶已登入應用程式，資料就會保持不變。應用程式防護原則可用來防止將公司或學校帳戶資料傳輸至多重身分識別應用程式內的個人帳戶、其他應用程式內的個人帳戶或個人應用程式。

IMPORTANT

不論應用程式是否支援多重身分識別，只有單一「公司」身分識別可以套用Intune應用程式保護原則。

如需「個人」內容的範例，請考慮在 Word 中啟動新檔的使用者，這會被視為個人內容，因此Intune不會套用應用程式保護原則。將檔儲存在「公司」OneDrive帳戶之後，就會將其視為「公司」內容，並Intune套用應用程式保護原則。

請考慮下列工作或「公司」內容範例：

- 使用者會使用其工作帳戶來啟動OneDrive應用程式。在工作內容中，他們無法將檔案移至個人儲存位置。稍後，當他們使用OneDrive搭配其個人帳戶時，他們可以從個人OneDrive複製和移動資料，而不受限制。
- 使用者開始在Outlook應用程式中草擬電子郵件。一旦填入主旨或訊息本文，使用者就無法將 FROM 位址從工作內容切換到個人內容，因為主旨和訊息本文會受到應用程式保護原則的保護。

NOTE

Outlook具有「個人」和「公司」電子郵件的合併電子郵件檢視。在此情況下，Outlook應用程式會在啟動時提示輸入Intune PIN。

IMPORTANT

雖然 Edge 位於「公司」內容中，但使用者可以刻意將OneDrive「公司」內容檔案移至未知的個人雲端儲存位置。若要避免這種情況，請參閱[管理受限制的網站](#)，並設定 Edge 允許/封鎖的網站清單。

Intune應用程式 PIN

PIN) (個人識別碼是密碼，用來確認正確的使用者正在應用程式中存取組織的資料。

PIN 提示

當使用者即將存取「公司」資料時，Intune提示輸入使用者的應用程式 PIN。在 Word、Excel 或 PowerPoint 等多重身分識別應用程式中，當使用者嘗試開啟「公司」檔或檔案時，系統會提示他們輸入 PIN。在單一身分識別應用程式中，例如使用[Intune App Wrapping Tool](#)管理的企業營運應用程式，會在啟動時提示 PIN，因為[Intune SDK](#)知道

使用者在應用程式中的體驗一律為「公司」。

PIN 提示或公司認證提示頻率

IT 系統管理員可以在Intune管理主控台中) (分鐘後重新檢查存取需求, 以定義 Intune Intune應用程式保護原則設定。此設定會指定在裝置上檢查存取需求之前的時間量, 並再次顯示應用程式 PIN 畫面或公司認證提示。不過, 會影響使用者提示頻率的 PIN 重要詳細資料如下:

- **PIN 會在相同發行者的應用程式之間共用, 以改善可用性:**

在 iOS/iPadOS 上, 相同應用程式發行者的所有應用程式之間會共用一個應用程式 PIN。例如, 所有 Microsoft 應用程式都會共用相同的 PIN。在 Android, 所有應用程式之間會共用一個應用程式 PIN。

- **在裝置重新開機 後 (分鐘) 行為之後, 重新檢查存取需求:**

計時器會追蹤非使用狀態的分鐘數, 以決定下一次顯示Intune應用程式 PIN 或公司認證提示的時機。在 iOS/iPadOS 上, 計時器不會受到裝置重新開機的影響。因此, 裝置重新開機不會影響使用者在iOS/iPadOS 應用程式中處於非作用中的分鐘數, 且Intune PIN (或公司認證) 原則為目標。在Android時, 計時器會在裝置重新開機時重設。因此, Android具有INTUNE PIN (或公司認證) 原則的應用程式, 可能會提示應用程式 PIN 或公司認證提示, 無論裝置重新開機後「在 (分鐘後重新檢查存取需求)」設定值為何。

- **與 PIN 相關聯之計時器的滾動本質:**

一旦輸入 PIN 以存取應用程式 (應用程式 A), 且應用程式離開前景 (裝置上的主要輸入焦點), 該 PIN 的計時器就會重設。共用此 PIN 的任何應用程式 (應用程式 B) 都不會提示使用者輸入 PIN, 因為計時器已重設。再次符合「在 (分鐘之後重新檢查存取需求)」值之後, 就會再次顯示提示。

針對iOS/iPadOS 裝置, 即使 PIN 是從不同發行者共用的應用程式, 當重新檢查 (分鐘之後的存取需求時, 也會再次顯示提示,) 值再次符合不是主要輸入焦點的應用程式。因此, 例如, 使用者擁有來自發行者 X 的應用程式 A 和發行者 Y 的應用程式 B, 而這兩個應用程式共用相同的 PIN。使用者著重于應用程式 A (前景), 並將應用程式 B 最小化。在 (分鐘後重新檢查存取需求之後,) 值符合, 且使用者切換至應用程式 B, 則需要 PIN。

NOTE

若要更頻繁地驗證使用者的存取需求, (也就是 PIN 提示), 特別是針對經常使用的應用程式, 建議您降低[在 (分鐘後重新檢查存取需求)] 設定的值。

適用於 Outlook 和 OneDrive 的內建應用程式 PIN

Intune PIN 會根據非活動計時器運作, () (分鐘後重新檢查存取需求) 的值。因此, Intune PIN 提示會與Outlook 和OneDrive的內建應用程式 PIN 提示分開顯示, 這些提示通常會與應用程式的啟動系統結。如果使用者同時收到這兩個 PIN 提示, 預期的行為應該是Intune PIN 優先。

Intune PIN 安全性

PIN 可用來只允許正確的使用者存取其組織在應用程式中的資料。因此, 使用者必須先使用其公司或學校帳戶登入, 才能設定或重設其Intune應用程式 PIN。此驗證是由Azure Active Directory透過安全權杖交換來處理, 對Intune SDK而言並不透明。從安全性觀點來看, 保護公司或學校資料的最佳方式是加密資料。加密與應用程式 PIN 無關, 而是它自己的應用程式保護原則。

防範暴力密碼破解攻擊和Intune PIN

作為應用程式 PIN 原則的一部分, IT 系統管理員可以設定使用者在鎖定應用程式之前, 可以嘗試驗證其 PIN 的次數上限。達到嘗試次數之後, Intune SDK可以抹除應用程式中的「公司」資料。

Intune PIN 和選擇性抹除

在 iOS/iPadOS 上, 應用層級 PIN 資訊會儲存在具有相同發行者之應用程式之間共用的金鑰鏈中, 例如所有第一方 Microsoft 應用程式。此 PIN 資訊也會系結至使用者帳戶。選擇性抹除一個應用程式不應影響不同的應用程式。

例如, 已登入使用者的Outlook PIN 集會儲存在共用金鑰鏈中。當使用者登入 Microsoft) 所發佈的OneDrive (時, 他們會看到與Outlook相同的 PIN 碼, 因為它使用相同的共用金鑰鏈。登出Outlook或抹除Outlook中的使用者資料時, Intune SDK 不會清除該金鑰鏈, 因為OneDrive可能仍在該 PIN。因此, 選擇性抹除不會清除該共用金鑰鏈, 包括 PIN。即使裝置上只有發行者有一個應用程式, 此行為仍維持不變。

由於 PIN 是在具有相同發行者的應用程式之間共用，因此，如果抹除移至單一應用程式，Intune SDK 並不知道裝置上是否有任何其他應用程式具有相同的發行者。因此，Intune SDK 不會清除 PIN，因為它可能仍可用於其他應用程式。預期是，當最後一個來自該發行者的應用程式最終會在某些作業系統清理過程中移除時，應該抹除應用程式 PIN。

如果您觀察到在某些裝置上抹除 PIN，可能會發生下列情況：因為 PIN 系統至身分識別，如果使用者在抹除之後使用不同的帳戶登入，系統會提示他們輸入新的 PIN。不過，如果他們使用先前現有的帳戶登入，儲存在金鑰鏈中的 PIN 就已經可以用來登入。

在來自相同發行者的應用程式上設定 PIN 兩次？

iOS/iPadOS 上的 MAM (目前允許具有英數位元和特殊字元的應用層級 PIN，(稱為「密碼」)，這需要應用程式 (例如 WXP、Outlook、Managed Browser Yammer) 參與，才能整合 [iOS 的 Intune SDK](#)。如果沒有，目標應用程式的密碼設定將不會正確強制執行。這是 Intune SDK for iOS v 中發行的功能。7.1.12。

為了支援這項功能，並確保與舊版 Intune SDK for iOS/iPadOS 的回溯相容性，7.1.12+ 中 (數值或密碼) 的所有 PIN 都會與舊版 SDK 中的數值 PIN 分開處理。Intune SDK for iOS 14.6.0 版中引進了另一項變更，導致 14.6.0+ 中的所有 PIN 都與舊版 SDK 中的任何 PIN 分開處理。

因此，如果裝置的應用程式在 7.1.12 之前和 7.1.12 之前具有適用於 iOS 版本的 Intune SDK，且 7.1.12 之後是來自相同發行者 (或 14.6.0 之前的版本，且在 14.6.0 之後)，則必須設定兩個 PIN。每個應用程式) 的兩個 PIN (以任何方式都不相關 (亦即，它們必須遵守套用至應用程式) 的應用程式保護原則。因此，*只有在* 應用程式 A 和 B 套用與 PIN) (相同的原則時，使用者才能設定相同的 PIN 兩次。

此行為專屬於使用 Intune Mobile App Management 啟用的 iOS/iPadOS 應用程式上的 PIN。經過一段時間後，當應用程式採用較新版本的 Intune SDK for iOS/iPadOS 時，必須在同一個發行者的應用程式上設定 PIN 兩次就變得較不成問題。如需範例，請參閱下列附注。

NOTE

例如，如果應用程式 A 是以 7.1.12 之前的版本建置，(或 14.6.0)，而應用程式 B 的版本大於或等於 7.1.12 (或來自相同發行者的 14.6.0)，如果兩者都安裝在 iOS/iPadOS 裝置上，終端使用者就必須分別設定 A 和 B 的 PIN。如果已在裝置上安裝 SDK 7.1.9 版 (或 14.5.0) 的應用程式 C，它會與應用程式 A 共用相同的 PIN。使用 7.1.14 (或 14.6.2) 建置的應用程式 D 會與應用程式 B 共用相同的 PIN。

如果裝置上只安裝應用程式 A 和 C，則必須設定一個 PIN。如果裝置上只安裝應用程式 B 和 D，則適用相同的方式。

應用程式資料加密

IT 系統管理員可以部署需要加密應用程式資料的應用程式保護原則。作為原則的一部分，IT 系統管理員也可以指定何時加密內容。

如何Intune資料加密程式

如需[加密應用程式保護原則設定](#)的詳細資訊，請參閱[Android應用程式保護原則設定](#)和[iOS/iPadOS 應用程式保護原則設定](#)。

加密的資料

只有標示為「公司」的資料會根據 IT 系統管理員的應用程式保護原則進行加密。資料來源自商務位置時會被視為「公司」。針對Office應用程式，Intune將下列專案視為商務位置：

- 電子郵件 (Exchange)
- 具有商務用 OneDrive帳戶) 的雲端儲存體 (OneDrive應用程式)

針對由[Intune App Wrapping Tool](#)管理的企業營運應用程式，所有應用程式資料都會視為「公司」。

選擇性抹除

從遠端抹除資料

Intune可以使用三種不同的方式抹除應用程式資料：

- 完整裝置抹除
- MDM 的選擇性抹除
- MAM 選擇性抹除

如需 MDM 遠端抹除的詳細資訊，請參閱 [使用抹除或淘汰來移除裝置](#)。如需使用 MAM 選擇性抹除的詳細資訊，請參閱 [淘汰動作](#) 和 [如何只抹除應用程式中的公司資料](#)。

完整裝置抹除 會將裝置還原為原廠預設設定，以從 **裝置** 移除所有使用者資料和設定。裝置會從Intune中移除。

NOTE

只有向Intune行動裝置管理 (MDM) 註冊的裝置上，才能完成 MDM 的完整裝置抹除和選擇性抹除。

MDM 的選擇性抹除

請參閱 [移除裝置 - 淘汰](#) 以閱讀移除公司資料的相關資訊。

MAM 的選擇性抹除

MAM 的選擇性抹除只會從應用程式移除公司應用程式資料。要求是使用Intune來起始。若要瞭解如何起始抹除要求，請參閱 [如何只抹除應用程式中的公司資料](#)。

如果使用者在起始選擇性抹除時使用應用程式，[Intune SDK](#)會每隔 30 分鐘檢查一次Intune MAM 服務的選擇性抹除要求。它也會在使用者第一次啟動應用程式時檢查選擇性抹除，並使用其公司或學校帳戶登入。

當內部部署 (內部部署) 服務無法與Intune保護的應用程式搭配運作時

Intune應用程式保護取決於使用者的身分識別，才能在應用程式與[Intune SDK](#)之間保持一致。保證的唯一方法是透過新式驗證。在某些情況下，應用程式可能會使用內部部署組態，但它們既不一致也不保證。

從受控應用程式開啟 Web 連結的安全方式

IT 系統管理員可以部署和設定[Microsoft Edge](#)的應用程式保護原則，這是一種可透過Intune輕鬆管理的網頁瀏覽器。IT 系統管理員可以要求使用受管理瀏覽器開啟Intune管理應用程式中的所有 Web 連結。

iOS裝置的應用程式防護體驗

裝置指紋或臉部識別碼

Intune應用程式保護原則只允許控制Intune授權使用者的應用程式存取權。控制應用程式存取的其中一種方式是在支援的裝置上要求 Apple 的觸控識別碼或臉部識別碼。Intune實作行為，如果裝置的生物特徵辨識資料庫有任何變更，Intune在符合下一個閒置逾時值時提示使用者輸入 PIN。生物特徵辨識資料的變更包括新增或移除指紋或臉部。如果Intune使用者沒有 PIN 集，系統會引導他們設定Intune PIN。

此程式的目的是要繼續在應用程式內保護組織的資料，並在應用層級受到保護。這項功能僅適用於 iOS/iPadOS，而且需要整合 Intune SDK for iOS/iPadOS 9.0.1 版或更新版本的應用程式參與。必須整合 SDK，才能在目標應用程式上強制執行行為。這項整合會以滾動為基礎進行，且取決於特定的應用程式小組。部分參與的應用程式包括 WXP、Outlook、Managed Browser 和 Yammer。

iOS共用延伸模組

您可以使用 iOS/iPadOS 共用延伸模組，在非受控應用程式中開啟公司或學校資料，即使資料傳輸原則設定為僅限受管理的應用程式或沒有應用程式。Intune應用程式保護原則不需管理裝置，就無法控制iOS/iPadOS 共用擴充功能。因此，Intune在 *應用程式外部共用「公司」資料之前，先將資料加密*。您可以嘗試在受控應用程式外部開啟「公司」檔案，以驗證此加密行為。檔案應加密，且無法在受控應用程式外部開啟。

通用連結支援

根據預設，Intune應用程式保護原則會防止存取未經授權的應用程式內容。在 iOS/iPadOS 中，有使用[通用連結](#)開啟特定內容或應用程式的功能。

使用者可以在 Safari 中流覽應用程式的通用連結，然後選取 [在新索引卷標中開啟] 或 [開啟]，以停用應用程

式的通用連結。若要使用通用連結與Intune應用程式保護原則，請務必重新啟用通用連結。使用者必須在長按對 < 應的連結之後，在 Safari 中執行開啟應用程式 **名稱**>。這應該會提示任何其他受保護的應用程式將所有通用連結路由傳送至裝置上受保護的應用程式。

同一組應用程式和使用者的多個Intune應用程式保護存取設定

Intune使用者裝置嘗試從其公司帳戶存取目標應用程式時，存取的應用程式保護原則會以特定順序套用。一般而言，抹除會優先，後面接著區塊，然後是可關閉的警告。例如，如果適用於特定使用者/應用程式，則會在封鎖使用者存取的最小iOS/iPadOS 作業系統設定之後套用警告使用者更新其iOS/iPadOS 版本的最小iOS/iPadOS 作業系統設定。因此，在 IT 系統管理員將最小iOS作業系統設定為 11.0.0.0，而最小iOS作業系統 (警告只會) 為 11.1.0.0 的案例中，當嘗試存取應用程式的裝置在 iOS 10 時，使用者會因為最小iOS作業系統版本的更嚴格設定而封鎖，而導致封鎖存取。

處理不同類型的設定時，Intune SDK 版本需求會優先，然後是應用程式版本需求，後面接著iOS/iPadOS 作業系統版本需求。然後，會檢查所有類型設定以相同順序出現的任何警告。我們建議您只在Intune產品小組提供基本封鎖案例的指引下，才設定Intune SDK 版本需求。

Android裝置的應用程式防護體驗

NOTE

Intune受控Android Enterprise專用裝置不支援應用程式防護原則。如果您Android Enterprise專用裝置上的使用者已針對另一部裝置套用應用程式原則，則您會想要採取下列步驟：

1. 請確定您想要的裝置僅Intune受管理的專用裝置。如果裝置是由協力廠商 MDM 提供者管理，則封鎖原則不會生效。
2. 確定公司入口網站安裝在專用裝置上。這是 APP 封鎖原則生效的必要專案。在專用裝置上公司入口網站應用程式不需要使用者互動，即可封鎖 APP 功能，因此不需要讓公司入口網站應用程式可供終端使用者啟動。公司入口網站只需要安裝在裝置上即可。例如，您不需要在受控主畫面上列出它。

請注意，在非專用裝置上以 APP 原則為目標的使用者將不會受到影響。

Microsoft Teams Android裝置

Microsoft Teams Android裝置上的Teams應用程式不支援 APP (不會透過公司入口網站應用程式) 接收原則。這表示應用程式保護原則設定不會套用至Microsoft Teams Android裝置上的Teams。如果您已針對這些裝置設定應用程式保護原則，請考慮建立一組Teams裝置使用者，並將該群組從相關的應用程式保護原則中排除。此外，請考慮修改Intune註冊原則、條件式存取原則和Intune合規性原則，使其具有支援的設定。如果您無法變更現有的原則，則必須 [裝置篩選器](#)設定 (排除)。根據現有的條件式存取組態確認每個設定，並Intune合規性原則，以瞭解您是否有不支援的設定。如需相關資訊，請參閱 [Microsoft Teams 會議室](#) 和 [Teams Android 裝置的支援條件式存取和Intune裝置合規性原則](#)。如需Microsoft Teams 會議室的相關資訊，請參閱[Microsoft Teams 會議室的條件式存取和Intune合規性](#)。

裝置生物特徵辨識驗證

針對支援生物特徵辨識驗證的Android裝置，您可以允許終端使用者使用指紋或臉部解除鎖定，視其Android裝置支援的內容而定。您可以設定是否可以使用指紋以外的所有生物特徵辨識類型來進行驗證。請注意，指紋和臉部解除鎖定僅適用於製造來支援這些生物特徵辨識類型的裝置，並執行正確的Android版本。指紋需要Android 6 和更新版本，而且臉部解除鎖定需要Android 10 和更高版本。

公司入口網站應用程式和Intune應用程式保護

大部分的應用程式保護功能都內建在公司入口網站應用程式中。即使一律 *需要* 公司入口網站應用程式，也不需要註冊裝置。針對行動應用程式管理 (MAM)，終端使用者只需要在裝置上安裝公司入口網站應用程式即可。

同一組應用程式和使用者的多個Intune應用程式保護存取設定

Intune使用者裝置嘗試從其公司帳戶存取目標應用程式時，存取的應用程式保護原則會以特定順序套用。一般而言，區塊會優先，然後是可關閉的警告。例如，如果適用於特定使用者/應用程式，則會在封鎖使用者存取的最小

Android修補程式版本設定之後，套用警告使用者進行修補程式升級的最小Android修補程式版本設定。因此，在IT系統管理員將最小Android修補程式版本設定為 2018-03-01 和最小Android修補程式版本 (警告只會) 至 2018-02-01 的案例中，當嘗試存取應用程式的裝置位於修補程式版本 2018-01-01 時，會根據最小Android修補程式版本的更嚴格設定來封鎖終端使用者，進而導致封鎖存取。

處理不同類型的設定時，應用程式版本需求會優先，後面接著Android作業系統版本需求和Android修補程式版本需求。然後，會檢查所有類型設定以相同順序出現的任何警告。

Intune應用程式保護原則和適用於Android裝置的 Google SafetyNet 證明

Intune應用程式保護原則可讓系統管理員要求使用者裝置通過適用於Android裝置的 Google SafetyNet 證明。新的Google Play服務判斷會在Intune服務所決定的間隔向 IT 系統管理員報告。由於負載，服務呼叫的頻率會受到節流處理，因此此值會在內部維護且無法設定。針對 Google SafetyNet 證明設定的任何 IT 系統管理員設定動作，都會根據條件式啟動時最後回報給Intune服務的結果來採取。如果沒有資料，則會根據沒有其他條件式啟動檢查失敗而允許存取，Google Play服務「往返」來判斷證明結果會從後端開始，並在裝置失敗時以非同步方式提示使用者。如果有過時的資料，將會根據最後回報的結果封鎖或允許存取，同樣地，判斷證明結果的Google Play服務「往返」將會開始，並在裝置失敗時以非同步方式提示使用者。

Intune應用程式保護原則和適用於Android裝置的 Google 驗證應用程式 API

Intune應用程式防護原則提供功能，讓系統管理員要求使用者裝置透過 Google 的驗證應用程式 API 傳送訊號以Android裝置。如何執行這項操作的指示會因裝置而稍有不同。一般程式牽涉到移至Google Play 商店，然後按一下 [我的應用程式] & 遊戲，按一下最後一個應用程式掃描的結果，這會帶您進入 [播放保護] 功能表。請確定已開啟 [掃描裝置是否有安全性威脅] 的切換開關。

Google 的 SafetyNet 證明 API

Intune利用 Google Play Protect SafetyNet API，將新增至我們現有的未註冊裝置根偵測檢查。Google 已開發並維護此 API 集合，讓Android應用程式在不想讓應用程式在根目錄裝置上執行時採用。例如，Android Pay 應用程式已納入此專案。雖然 Google 不會公開共用所發生的整個根偵測檢查，但我們預期這些 API 會偵測已破解其裝置的使用者。這些使用者接著可能會遭到封鎖而無法存取，或從已啟用原則的應用程式抹除其公司帳戶。檢查基本完整性 會告訴您裝置的一般完整性。具有竄改徵兆的根裝置、模擬器、虛擬裝置和裝置，會失敗基本完整性。檢查認證裝置&的基本完整性 會告訴您裝置與 Google 服務的相容性。只有經過 Google 認證的未修改裝置才能通過這項檢查。將會失敗的裝置包括下列專案：

- 不符合基本完整性的裝置
- 具有解除鎖定開機載入器的裝置
- 具有自訂系統映射/ROM 的裝置
- 製造商未申請或通過 Google 認證的裝置
- 具有直接從 Android 開放原始碼計畫來源檔案建置系統映射的裝置
- 具有 Beta/開發人員預覽系統映射的裝置

如需技術詳細資料，請參閱 [Google 關於 SafetyNet 證明的檔](#)。

SafetyNet 裝置證明設定和 [已越獄/Root 破解的裝置] 設定

Google Play保護的 SafetyNet API 檢查會要求終端使用者在線上，在判斷證明結果的「往返」執行期間最長。如果終端使用者離線，IT系統管理員仍可預期會從 已越獄/Root 破解的裝置 設定強制執行結果。也就是說，如果終端使用者離線的時間太長，離線寬限期 值就會生效，而且一旦達到該計時器值，所有對公司或學校資料的存取都會遭到封鎖，直到有網路存取可用為止。開啟這兩個設定可讓使用者裝置保持健全狀況的多層式方法，這在使用者存取行動裝置上的公司或學校資料時很重要。

Google Play保護 API 和Google Play Services

運用Google Play保護 API 的應用程式保護原則設定需要Google Play Services才能運作。SafetyNet 裝置證明和應用程式設定的威脅掃描 都需要 Google 決定的Google Play Services版本才能正常運作。由於這些是屬於安全性領域的設定，因此，如果終端使用者以這些設定為目標，且不符合適當版本的Google Play Services或無法存取Google Play Services，則會封鎖使用者。

後續步驟

[如何使用 Microsoft Intune 建立及部署應用程式保護原則](#)

[Android 應用程式保護原則設定的可用 Microsoft Intune](#)

[iOS/iPadOS 應用程式保護原則設定與 Microsoft Intune](#)

使用應用程式防護原則的資料保護架構

2022/9/27 •

隨著更多組織實行行動裝置策略來存取公司或學校資料，防止資料外泄變得至關重要。Intune的行動應用程式管理解決方案可防止資料外泄，請參閱應用程式 (應用程式保護原則)。APP 是確保組織資料安全或包含在受控應用程式中的規則，不論裝置是否已註冊。如需詳細資訊，請參閱[應用程式防護原則概觀](#)。

設定應用程式保護原則時，各種設定和選項的數目可讓組織根據其特定需求量身打造保護。由於此彈性，實作完整案例所需的原則設定排列可能不明顯。為了協助組織排定用戶端端點強化工作的優先順序，Microsoft 為[Windows 10中的安全性設定](#)引進了新的分類法，Intune針對其應用程式資料保護架構運用類似的分類法來管理行動應用程式。

應用程式資料保護組態架構會組織成三個不同的組態案例：

- 層級 1 企業基本資料保護 – Microsoft 建議將此設定作為企業裝置的最低資料保護設定。
- 層級 2 企業增強型資料保護 – Microsoft 建議針對使用者存取敏感或機密資訊的裝置使用此設定。此設定適用於大部分存取公司或學校資料的行動使用者。某些控制項可能會影響使用者體驗。
- 層級 3 企業高資料保護 – Microsoft 建議針對組織所執行且具有較大或更複雜安全性小組的裝置，或針對具有唯一高風險的特定使用者或群組，(處理未經授權洩漏會對組織) 造成大量資料遺失之高敏感性資料的使用者進行這項設定。可能以資金高且複雜的敵人為目標的組織應該想要進行此設定。

APP Data Protection Framework 部署方法

如同任何新軟體、功能或設定的部署，Microsoft 建議您在部署 APP 資料保護架構之前，先投資通道方法來測試驗證。定義部署更新步調通常是一次性事件 (或至少不常)，但 IT 應該重新流覽這些群組，以確保排序仍然正確。

Microsoft 建議針對 APP 資料保護架構使用下列部署通道方法：

品質保證	進入生產階段前租用戶	行動功能擁有者、安全性、風險評定、隱私權、UX	功能案例驗證、草稿文件	0-30 天
預覽	生產租用戶	行動功能擁有者、UX	終端使用者案例驗證、使用者互動文件	7-14 天, 品質保證後
生產環境	生產租用戶	行動功能擁有者、IT 支援人員	不適用	7 天到數週, 預覽後

如上表所示，應用程式保護原則的所有變更都應該先在生產前環境中執行，以瞭解原則設定的含意。測試完成後，變更就可以移至生產環境，並套用至生產使用者的子集，通常是 IT 部門和其他適用的群組。最後，您可以對行動使用者社群的其餘部分完成推出。根據變更的影響程度而定，推出至生產環境可能需要較長的時間。如果沒有使用者影響，變更應該會快速推出，而如果變更造成使用者影響，則推出可能需要變慢，因為需要將變更傳達給使用者母體。

測試 APP 的變更時，請留意 [傳遞時間](#)。您可以監視指定使用者的 APP 傳遞狀態。如需詳細資訊，請參閱[如何監視應用程式保護原則](#)。

您可以使用 Edge 和 URL `about:Intunehelp`，在裝置上驗證每個應用程式的個別應用程式設定。如需詳細資訊，請參閱[檢閱用戶端應用程式保護記錄](#)和[使用適用於 iOS 和 Android 的 Edge 來存取受控應用程式記錄](#)。

APP 資料保護架構設定

應為適用的應用程式啟用下列應用程式保護原則設定，並指派給所有行動使用者。如需每個原則設定的詳細資訊，請參閱 [iOS 應用程式保護原則設定](#) 和 [Android 應用程式保護原則設定](#)。

Microsoft 建議您檢閱和分類使用案例，然後使用該層級的規範指引來設定使用者。如同任何架構，對應層級內的設定可能需要根據組織的需求進行調整，因為資料保護必須評估威脅環境、風險偏好，以及對可用性的影響。

系統管理員可以藉由匯入範例 [Intune 應用程式防護原則設定架構 JSON 範本](#) 與 [Intune 的 PowerShell 腳本](#)，將下列設定層級納入其通道部署方法中，以進行測試和生產使用。

條件式存取原則

若要確保只有支援應用程式保護原則的應用程式才能存取公司或學校帳戶資料，需要 Azure Active Directory 條件式存取原則。這些原則會在 [條件式存取：需要核准的用戶端應用程式或應用程式保護原則](#) 中說明。

如需實作特定原則的步驟，請參閱 [條件式存取：需要核准的用戶端應用程式或應用程式保護原則](#)，以取得使用行動裝置核准的用戶端應用程式或 [應用程式保護](#) 原則。最後，實作 [封鎖舊版驗證](#) 中的步驟，以封鎖支援舊版驗證的 iOS 和 Android 應用程式。

NOTE

這些原則會利用授與控制 [要求已核准的用戶端應用程式](#) 和 [需要應用程式保護原則](#)。

要包含在應用程式保護原則中的應用程式

針對每個應用程式保護原則，核心 Microsoft Apps 群組會設為目標，其中包括下列應用程式：

- 銳利
- Excel
- Office
- OneDrive
- OneNote
- Outlook
- PowerPoint
- SharePoint
- Teams
- To Do
- Word

這些原則應包含其他根據商務需求的 Microsoft 應用程式、已整合組織內所使用之 Intune SDK 的其他協力廠商公用應用程式，以及已整合 [Intune SDK](#) (或已包裝) 的企業營運應用程式。

層級 1 企業基本資料保護

層級 1 是企業行動裝置的最低資料保護組態。此設定會藉由要求 PIN 存取公司或學校資料、加密公司或學校帳戶資料，以及提供選擇性抹除學校或公司資料的功能，來取代基本 Exchange Online 裝置存取原則的需求。不過，與 Exchange Online 裝置存取原則不同，下列應用程式保護原則設定會套用到原則中選取的所有應用程式，藉此確保資料存取受到行動訊息案例以外的保護。

層級 1 中的原則會強制執行合理的資料存取層級，同時將對使用者的影響降到最低，並在 Microsoft 端點管理員內建立應用程式保護原則時鏡像預設的資料保護和存取需求設定。

資料保護

功能	描述	平台	支援平台
資料傳輸	將組織資料備份到...	允許	iOS/iPadOS、Android
資料傳輸	將組織資料傳送至其他應用程式	所有應用程式	iOS/iPadOS、Android
資料傳輸	從其他應用程式接收資料	所有應用程式	iOS/iPadOS、Android
資料傳輸	限制應用程式之間的剪下、複製和貼上	任何應用程式	iOS/iPadOS、Android
資料傳輸	協力廠商鍵盤	允許	iOS/iPadOS
資料傳輸	核准的鍵盤	不需要	Android
資料傳輸	螢幕擷取和 Google Assistant	允許	Android
加密	加密組織資料	需要	iOS/iPadOS、Android
加密	加密已註冊裝置上的組織資料	需要	Android
功能	同步處理應用程式與原生連絡人應用程式	允許	iOS/iPadOS、Android
功能	列印組織資料	允許	iOS/iPadOS、Android
功能	限制與其他應用程式的 Web 內容傳輸	任何應用程式	iOS/iPadOS、Android
功能	組織資料通知	允許	iOS/iPadOS、Android

存取需求

功能	描述	平台	支援平台
用於存取的 PIN	需要	iOS/iPadOS、Android	
PIN 類型	數值	iOS/iPadOS、Android	
簡單 PIN	允許	iOS/iPadOS、Android	
選取 PIN 長度下限	4	iOS/iPadOS、Android	
用於存取 iOS 8+/iPadOS (的觸控識別碼, 而不是 PIN)	允許	iOS/iPadOS	
逾時後使用 PIN 覆寫生物特徵辨識	需要	iOS/iPadOS、Android	
活動 (分鐘的逾時)	720	iOS/iPadOS、Android	

「	「	「	「
用於存取 iOS 11+/iPadOS (的臉部識別碼, 而不是 PIN)	允許	iOS/iPadOS	
用於存取的生物特徵辨識而非 PIN	允許	iOS/iPadOS、Android	
在天數之後重設 PIN	否	iOS/iPadOS、Android	
選取要維護的先前 PIN 值數目	0	Android	
設定裝置 PIN 時的應用程式 PIN	需要	iOS/iPadOS、Android	如果裝置已在Intune註冊, 如果系統管理員透過裝置合規性政策強制執行強式裝置 PIN, 則可以考慮將此設定為「不需要」。
用於存取的公司或學校帳號憑證	不需要	iOS/iPadOS、Android	
在閒置 (分鐘後重新檢查存取需求)	30	iOS/iPadOS、Android	

條件式啟動

「	「	「	「	「
應用程式條件	PIN 嘗試次數上限	5 / 重設 PIN	iOS/iPadOS、Android	
應用程式條件	離線寬限期	720 / 封鎖存取 (分鐘)	iOS/iPadOS、Android	
應用程式條件	離線寬限期	90 / 抹除資料 (天)	iOS/iPadOS、Android	
裝置條件	已越獄/Root 破解的裝置	N/A / 封鎖存取	iOS/iPadOS、Android	

「	「「「	「/「	「	「
裝置條件	SafetyNet 裝置證明	基本完整性和認證的裝置/封鎖存取	Android	此設定會在使用者裝置上設定 Google 的 SafetyNet 證明。基本完整性會驗證裝置的完整性。具有竄改徵兆的根裝置、模擬器、虛擬裝置和裝置，會失敗基本完整性。 基本完整性和認證的裝置會驗證裝置與 Google 服務的相容性。只有經過 Google 認證的未修改裝置才能通過這項檢查。
裝置條件	需要對應用程式進行威脅掃描	N/A / 封鎖存取	Android	此設定可確保已針對終端使用者裝置開啟 Google 的驗證應用程式掃描。如果設定，使用者將會遭到封鎖而無法存取，直到他們在其 Android 裝置上開啟 Google 的應用程式掃描為止。
裝置條件	需要裝置鎖定	低/警告	Android	此設定可確保 Android 裝置具有符合最低密碼需求的裝置密碼。

層級 2 企業增強型資料保護

層級 2 是建議作為標準的資料保護設定，適用於使用者存取更敏感性資訊的裝置。這些裝置是現今企業中的自然目標。這些建議不會假設有大量高技能的安全性從業人員，因此大部分的企業組織都應該能夠存取這些建議。此組態會藉由限制資料傳輸案例和要求最低作業系統版本，來擴充層級 1 中的設定。

層級 2 中強制執行的原則設定包含針對層級 1 建議的所有原則設定，但只會列出下列已新增或變更的設定，以實作比層級 1 更多的控制項和更複雜的設定。雖然這些設定可能會對使用者或應用程式產生稍微較高的影響，但其強制執行的資料保護層級更符合使用者在行動裝置上存取敏感性資訊所面臨的風險。

資料保護

「	「「「	「	「	「
資料傳輸	將組織資料備份到...	封鎖	iOS/iPadOS、Android	

【】	【】	【】	【】	【】
資料傳輸	將組織資料傳送至其他應用程式	受原則管理的應用程式	iOS/iPadOS、Android	使用 iOS/iPadOS, 系統管理員可以將此值設定為「受原則管理的應用程式」、「具有 OS 共用的原則受控應用程式」或「具有開啟/共用篩選的原則受控應用程式」。 當裝置也向 Intune註冊時, 可以使用具有 OS 共用的原則受控應用程式。此設定可讓您將資料傳輸至其他受原則管理的應用程式, 以及將檔案傳輸至由Intune管理的其他應用程式。 使用 [開啟/共用] 篩選的原則受控應用程式會篩選 OS [開啟/共用] 對話方塊, 只顯示受原則管理的應用程式。 如需詳細資訊, 請參閱 iOS 應用程式保護原則設定。
資料傳輸	選取要豁免的應用程式	Default / skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services;	iOS/iPadOS	
資料傳輸	儲存組織資料的複本	封鎖	iOS/iPadOS、Android	
資料傳輸	允許使用者將複本儲存至選取的服務	商務用 OneDrive、SharePoint Online、相片媒體櫃	iOS/iPadOS、Android	
資料傳輸	將電信資料傳輸至	任何撥號程式應用程式	iOS/iPadOS、Android	
資料傳輸	限制應用程式之間的剪下、複製和貼上	貼入的原則受控應用程式	iOS/iPadOS、Android	
資料傳輸	螢幕擷取和 Google Assistant	封鎖	Android	

功能	限制與其他應用程式的 Web 內容傳輸	Microsoft Edge	iOS/iPadOS、Android	
功能	組織資料通知	封鎖組織資料	iOS/iPadOS、Android	如需支援此設定的應用程式清單, 請參閱 iOS 應用程式保護原則設定 和 Android 應用程式保護原則設定 。

條件式啟動

功能	限制與其他應用程式的 Web 內容傳輸	Microsoft Edge	iOS/iPadOS、Android	
應用程式條件	已停用帳戶	N/A / 封鎖存取	iOS/iPadOS、Android	
裝置條件	最低 OS 版本	格式: <i>Major.Minor.Build</i> 範例: 14.8 / 封鎖存取	iOS/iPadOS	Microsoft 建議設定最低 iOS 主要版本, 以符合 Microsoft 應用程式支援的 iOS 版本。Microsoft 應用程式支援 N-1 方法, 其中 N 是目前的 iOS 主要發行版本。針對次要和組建版本值, Microsoft 建議確保裝置具有個別的安全性更新是最新的。如需 Apple 的最新建議, 請參閱 Apple 安全性更新
裝置條件	最低 OS 版本	格式: <i>Major.Minor</i> 範例: 9.0 / 封鎖存取	Android	Microsoft 建議設定最低 Android 主要版本, 以符合 Microsoft 應用程式支援的 Android 版本。符合 Android Enterprise 建議需求的 OEM 和裝置必須支援目前的出貨版本 + 一個字母升級。目前, Android 針對知識工作者建議使用 Android 9.0 和更新版本。如需 Android 的最新建議, 請參閱 Android Enterprise 建議 需求

II	IIII	I/II	II	II
裝置條件	最小修補程式版本	格式: YYYY-MM-DD 範例: 2020-01-01 / 封鎖存取	Android	Android 裝置可以接收每月安全性修補程式, 但版本取決於 OEM 和/或貨運公司。組織應該確保已部署的 Android 裝置在實作此設定之前, 確實會收到安全性更新。如需最新的修補程式版本, 請參閱 Android 安全性佈告欄 。
裝置條件	必要的 SafetyNet 評估類型	硬體支援的金鑰	Android	硬體支援的證明藉由利用稱為 Hardware Backed 的新評估類型, 來增強現有的 SafetyNet 證明服務檢查, 提供更健全的根偵測, 以回應較新類型的根工具和方法, 這些工具和方法永遠無法由軟體專用解決方案可靠地偵測。 正如其名稱所示, 硬體支援的證明會利用隨附于 Android 8.1 和更新版本安裝之裝置的硬體型元件。從舊版 Android 升級至 Android 8.1 的裝置不太可能有硬體支援證明所需的硬體型元件。雖然從 Android 8.1 隨附的裝置開始應該廣泛支援此設定, 但 Microsoft 強烈建議您在廣泛啟用此原則設定之前, 先個別測試裝置。
裝置條件	需要裝置鎖定	中型/區塊存取	Android	此設定可確保 Android 裝置具有符合最低密碼需求的裝置密碼。

層級 3 企業高資料保護

層級 3 是建議作為標準的資料保護組態, 適用於具有大型和複雜安全性組織的組織, 或是針對會被攻擊者唯一設為目標的特定使用者和群組。這類組織通常會以資金高且複雜的敵人為目標, 因此值得說明其他條件約束和控制項。此設定會藉由限制其他資料傳輸案例、增加 PIN 設定的複雜度, 以及新增行動威脅偵測, 來擴充層級 2 中的設定。

層級 3 中強制執行的原則設定包含針對層級 2 建議的所有原則設定, 但只會列出下列已新增或變更的設定, 以實作比層級 2 更複雜的控制項和更複雜的設定。這些原則設定可能會對使用者或應用程式造成重大影響, 強制

執行與目標群組織所面臨風險相符的安全性層級。

資料保護

功能	目標群組織	風險	平台	說明
資料傳輸	將電信資料傳輸至	任何受原則管理的撥號程式應用程式	Android	系統管理員也可以藉由選取 撥號程式 ，並提供撥號程式名稱值，將此設定設定為使用不支援應用程式保護原則的撥號程式。
資料傳輸	將電信資料傳輸至	特定撥號程式應用程式	iOS/iPadOS	
資料傳輸	撥號程式應用程式 URL 配置	<i>replace_with_dialer_app_url_scheme</i>	iOS/iPadOS	在 iOS/iPadOS 上，此值必須取代為所使用自訂撥號程式應用程式的 URL 配置。如果 URL 配置未知，請連絡應用程式開發人員以取得詳細資訊。如需 URL 配置的詳細資訊，請 參閱定義應用程式的自訂 URL 配置 。
資料傳輸	從其他應用程式接收資料	受原則管理的應用程式	iOS/iPadOS、Android	
資料傳輸	將資料開啟至組織檔	封鎖	iOS/iPadOS、Android	
資料傳輸	允許使用者從選取的服務開啟資料	商務用 OneDrive、SharePoint、相機、相片媒體櫃	iOS/iPadOS、Android	如需相關資訊，請參閱 Android 應用程式保護原則設定 和 iOS 應用程式保護原則設定 。
資料傳輸	協力廠商鍵盤	封鎖	iOS/iPadOS	在 iOS/iPadOS 上，這會封鎖所有協力廠商鍵盤在應用程式內運作。
資料傳輸	核准的鍵盤	需要	Android	
資料傳輸	選取要核准的鍵盤	<i>新增/移除鍵盤</i>	Android	使用 Android 時，必須選取鍵盤，才能根據您部署的 Android 裝置來使用。
功能	列印組織資料	封鎖	iOS/iPadOS、Android	
裝置條件	需要裝置鎖定	高/區塊存取	Android	此設定可確保 Android 裝置具有符合最低密碼需求的裝置密碼。

存取需求

⌘	⌘	⌘
簡單 PIN	封鎖	iOS/iPadOS、Android
選取 PIN 長度下限	6	iOS/iPadOS、Android
在天數之後重設 PIN	是	iOS/iPadOS、Android
天數	365	iOS/iPadOS、Android
類別 3 Biometrics (Android 9.0+)	需要	Android
在生物特徵辨識更新之後使用 PIN 覆寫生物特徵辨識	需要	Android

條件式啟動

⌘	⌘⌘⌘	⌘/⌘	⌘	⌘
裝置條件	已越獄/Root 破解的裝置	N/A / 抹除資料	iOS/iPadOS、Android	
裝置條件	允許的威脅層級上限	安全/封鎖存取	iOS/iPadOS、Android	您可以使用 Mobile Threat Defense 檢查未註冊的裝置是否有威脅。如需詳細資訊，請參閱 未註冊裝置的 Mobile Threat Defense。 如果裝置已註冊，則可以略過此設定，以便為已註冊的裝置部署 Mobile Threat Defense。如需詳細資訊，請參閱 已註冊裝置的 Mobile Threat Defense。
裝置條件	OS 版本上限	<i>格式: Major.Minor</i> <i>範例: 11.0 / 封鎖存取</i>	Android	Microsoft 建議設定 Android 主要版本上限，以確保不使用 Beta 或不支援的作業系統版本。如需 Android 的最新建議，請參閱 Android Enterprise 建議 需求

裝置條件	OS 版本上限	格式： <i>Major.Minor.Build</i> 範例：15.0 / 封鎖存取	iOS/iPadOS	Microsoft 建議設定 iOS/iPadOS 主要版本 上限，以確保不使用 Beta 或不支援的作業 系統版本。如需 Apple 的最新建議，請 參閱 Apple 安全性更新

後續步驟

系統管理員可以藉由匯入範例[Intune應用程式防護原則設定架構 JSON 範本](#)與[Intune的 PowerShell 腳本](#)，將上述設定層級納入其通道部署方法中以進行測試和生產使用。

另請參閱

- [如何使用 Microsoft Intune 建立及部署應用程式保護原則](#)
- [具有 Microsoft Intune 的可用 Android 應用程式保護原則設定](#)
- [可用的 iOS/iPadOS 應用程式保護原則設定與Microsoft Intune](#)

如何建立及部署應用程式保護原則

2022/9/27 •

瞭解如何 (應用程式) 為組織使用者建立及指派Microsoft Intune應用程式保護原則。本主題也說明如何對現有原則進行變更。

在您開始之前

應用程式防護原則可以套用至在裝置上執行的應用程式，這些應用程式可能由Intune管理。如需應用程式保護原則運作方式的詳細說明，以及Intune應用程式保護原則所支援的案例，請參閱[應用程式防護原則概觀](#)。

應用程式保護原則中可用的選項 (APP) 可讓組織根據其特定需求量身打造保護。對某些人而言，實作完整案例所需的原則設定可能不明顯。為了協助組織排定行動用戶端端點強化的優先順序，Microsoft 為其適用於 iOS 和 Android 行動應用程式管理的應用程式資料保護架構引進了分類法。

APP 資料保護架構會組織成三個不同的組態層級，每個層級會根據上一個層級來建置：

- **企業基本資料保護** (層級 1) 確保應用程式受到 PIN 保護並加密，並執行選擇性抹除作業。針對 Android 裝置，此層級會驗證 Android 裝置證明。這是一種進入層級設定，可在信箱原則Exchange Online提供類似的資料保護控制，並將 IT 和使用者母體引進 APP。
- **企業增強的資料保護** (層級 2) 引進 APP 資料外泄防護機制和最低 OS 需求。這是適用於大部分存取公司或學校資料之行動使用者的設定。
- **企業高資料保護** (層級 3) 引進進階資料保護機制、增強的 PIN 設定，以及 APP Mobile Threat Defense。此設定適用於存取高風險資料的使用者。

若要查看每個設定層級的特定建議，以及必須保護的最低應用程式，請[檢閱使用應用程式保護原則的資料保護架構](#)。

如果您要尋找已整合 Intune SDK 的應用程式清單，請參閱[Microsoft Intune受保護的應用程式](#)。

如需將貴組織的企業營運 (LOB) 應用程式新增至Microsoft Intune以準備應用程式保護原則的相關資訊，請參閱[將應用程式新增至Microsoft Intune](#)。

應用程式防護 iOS/iPadOS 和 Android 應用程式的原則

當您建立 iOS/iPadOS 和 Android 應用程式的應用程式保護原則時，您會遵循新式Intune程式流程，以產生新的應用程式保護原則。如需為 Windows 應用程式建立應用程式保護原則的相關資訊，請參閱[使用 Intune 建立和部署 Windows 資訊保護 \(WIP\) 原則](#)。

建立 iOS/iPadOS 或 Android 應用程式保護原則

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式] > [應用程式防護原則]。此選項會開啟 [應用程式防護原則](#) 詳細資料，您可以在其中建立新原則並編輯現有原則。
3. 選取 [建立原則]，然後選取 [iOS/iPadOS] 或 [Android]。[建立原則] 窗格隨即顯示。
4. 在 [基本] 頁面上，新增下列值：

I	II
名稱	此應用程式保護原則的名稱。

I	II
描述	[選擇性]此應用程式保護原則的描述。

[平台]**** 值是根據您在上方的選擇而設定。

Create policy

1 Basics

2 Apps

3 Data protection

4 Access requirements

5 Conditional launch

6 Assignments

7 Review + create

Name *

My Test Policy

Description

Platform

iOS/iPadOS

Previous

Next

5. 按 [下一步] 以顯示 [應用程式] 頁面。

[應用程式]**** 頁面可讓您選擇如何將此原則套用至不同裝置上的應用程式。您必須新增至少一個應用程式。

I/II	II
以所有裝置類型的應用程式為目標	使用此選項，將您的原則目標設為任何管理狀態裝置上的應用程式。選擇 [■] 以將特定裝置類型的應用程式設為目標。如需詳細資訊，請參閱 以裝置管理狀態為基礎的目標應用程式保護原則 。
裝置類型	使用此選項來指定此原則是否適用於 MDM 受控裝置或非受控裝置。針對 iOS/iPadOS APP 原則，請從 [■] 和受 [■] 裝置] 中選取。針對 Android 應用程式原則，請從 [■]、[Android ■■■] 和 [Android Enterprise] ■ 選取。
目標原則為	在 [■■■■] 下拉式方塊中，選擇將應用程式保護原則的目標設為 [■■■■]、[Microsoft Apps] 或 [■Microsoft Apps]。 ■■■■ 都包含已整合 Intune SDK 的所有 Microsoft 和合作夥伴應用程式。 - Microsoft Apps 包含已整合 Intune SDK 的所有 Microsoft 應用程式。 ■Microsoft Apps 包含下列應用程式：Edge、Excel、Office、OneDrive、OneNote、Outlook、PowerPoint、SharePoint、Teams、To Do 和 Word。 接下來，您可以選 ■ [■■■■]，以檢視受此原則影響的應用程式清單。

I/II	II
公用應用程式	如果您不想要選取其中一個預先定義的應用程式群組，您可以在 [目標原則要] 下拉式方塊中選 ■ [] ■ 選擇以個別應用程式為目標。按一下 [] 以選取要設為目標的公用應用程式。
自訂應用程式	如果您不想要選取其中一個預先定義的應用程式群組，您可以在 [目標原則要] 下拉式方塊中選 ■ [] ■ 選擇以個別應用程式為目標。按一下 [] ，以根據套件組合識別碼選取要設為目標的自訂應用程式。以相同原則中的所有公用應用程式為目標時，您無法選擇自訂應用程式。

您選取的應用程式 () 會出現在公用和自訂應用程式清單中。

NOTE

■ 是 Microsoft 的應用程式，以及常用於 Microsoft Intune 的合作夥伴。這些 Intune 受保護的應用程式會透過一組豐富的行動應用程式保護原則支援來啟用。如需詳細資訊，請參閱 [Microsoft Intune 受保護的應用程式](#)。自訂應用程式是已與 Intune SDK 整合或由 Intune App Wrapping Tool 包裝的 LOB 應用程式。如需詳細資訊，請參閱 [Microsoft Intune App SDK 概觀](#) 和 [準備應用程式保護原則的企業營運應用程式](#)。

6. 按 [下一步] 以顯示 [資料保護] 頁面。

此頁面提供資料外洩防護 (DLP) 控制項的設定，包括剪下、複製、貼上和另存新檔限制。這些設定決定使用者在套用此應用程式防護原則的應用程式中，如何與資料互動。

資料保護設定：

- iOS/iPadOS 資料保護 - 如需詳細資訊，請參閱 [iOS/iPadOS 應用程式保護原則設定 - 資料保護](#)。
- Android 資料保護 - 如需詳細資訊，請參閱 [Android 應用程式保護原則設定 - 資料保護](#)。

7. 按 [下一步] 以顯示 [存取需求] 頁面。

此頁面提供的設定，可讓您設定使用者必須符合的 PIN 和認證需求，才能在工作環境中存取應用程式。

存取需求設定：

- iOS/iPadOS 存取需求 - 如需詳細資訊，請參閱 [iOS/iPadOS 應用程式保護原則設定 - 存取需求](#)。
- Android 存取需求 - 如需詳細資訊，請參閱 [Android 應用程式保護原則設定 - 存取需求](#)。

8. 按 [下一步] 以顯示 [條件式啟動] 頁面。

此頁面提供的設定，可設定應用程式防護原則的登入安全性需求。選取 ****[設定]，然後輸入使用者必須符合的 ****[值]，才能登入您的公司應用程式。然後，選取您在使用者不符合需求時要採取的 ****[動作]。在某些情況下，單一設定可以設定多個動作。

條件式啟動設定：

- iOS/iPadOS 條件式啟動 - 如需詳細資訊，請參閱 [iOS/iPadOS 應用程式保護原則設定 - 條件式啟動](#)。
- Android 條件式啟動 - 如需詳細資訊，請參閱 [Android 應用程式保護原則設定 - 條件式啟動](#)。

9. 按 [下一步] 以顯示 [指派] 頁面。

[指派] 頁面可讓您將應用程式保護原則指派給使用者群組。您必須將原則套用至一組使用者，原則才會生效。

10. 按 [下一步：檢閱 + 建立] 以檢閱您為此應用程式保護原則輸入的值和設定。

11. 當您完成時，按一下 [建立] 以在 Intune 中建立應用程式保護原則。

TIP

只有在工作內容中使用應用程式時，才會強制執行這些原則設定。當終端使用者使用應用程式來執行個人工作時，不會受到這些原則的影響。請注意，當您建立新檔案時，它會被視為個人檔案。

IMPORTANT

應用程式保護原則可能需要一些時間才能套用至現有的裝置。套用應用程式保護原則時，終端使用者會在裝置上看到通知。套用連續存取規則之前，請先將您的應用程式保護原則套用至裝置。

終端使用者可以從 App Store 或 Google Play 下載應用程式。如需詳細資訊，請參閱：

- [適用於 Android 的 Managed 工作和學校應用程式](#)
- [當 iOS/iPadOS 應用程式受應用程式保護原則管理時，會發生什麼事](#)

變更現有原則

您可以編輯現有的原則，並將其套用至目標使用者。不過，當您變更現有的原則時，已登入應用程式的使用者將不會在八小時的期間內看到變更。

若要立即查看變更的影響，使用者必須登出應用程式，然後重新登入。

變更與原則相關聯的應用程式清單

1. 在 [應用程式防護原則] 窗格中，選取您想要變更的原則。
2. 在 [Intune 應用程式保護] 窗格中，選取 [屬性]。
3. 在標題為 [應用程式] 的區段旁，選取 [編輯]。
4. [應用程式]**** 頁面可讓您選擇如何將此原則套用至不同裝置上的應用程式。您必須新增至少一個應用程式。

目標	說明
以所有裝置類型的應用程式為目標	使用此選項，將您的原則目標設為任何管理狀態裝置上的應用程式。選擇 [■] 以將特定裝置類型的應用程式設為目標。此設定可能需要額外的應用程式設定。如需詳細資訊，請參閱 以裝置管理狀態為基礎的目標應用程式保護原則 。
裝置類型	使用此選項來指定此原則是否適用於 MDM 受控裝置或非受控裝置。針對 iOS/iPadOS APP 原則，請從 [■] 和受 [■] 裝置] 中選取。針對 Android 應用程式原則，請從 [■]、[Android ■■■] 和 [Android Enterprise] ■ 選取。
公用應用程式	在 [■■■] 下拉式方塊中，選擇將應用程式保護原則的目標設為 [■■■]、[Microsoft Apps] 或 [■Microsoft Apps]。接下來，您可以選 ■ [■■■■]，以檢視受此原則影響的應用程式清單。 如有需要，您可以按一下 [■■■■]，選擇以個別應用程式為目標。
自訂應用程式	按一下 [■■■■]，以根據套件組合識別碼選取要設為目標的自訂應用程式。

您選取的應用程式 () 會出現在公用和自訂應用程式清單中。

5. 按一下 [檢閱 + 建立] 以檢閱為此原則選取的應用程式。

6. 完成後，按一下 [儲存] 以更新應用程式保護原則。

變更使用者群組清單

1. 在 [應用程式防護原則] 窗格中，選取您想要變更的原則。
2. 在 [Intune 應用程式保護] 窗格中，選取 [屬性]。
3. 在標題為 [指派] 的區段旁，選取 [編輯]。
4. 若要將新的使用者群組新增至原則，請在 [包含] 索引標籤上選擇 [選取要包含的群組]，然後選取使用者群組。選擇 [選取] 以新增群組。
5. 若要排除使用者群組，請在 [排除] 索引標籤上選擇 [選取要排除的群組]，然後選取使用者群組。選擇 [選取] 以移除使用者群組。
6. 若要刪除先前新增的群組，請在 [包含] 或 [排除] 索引標籤上，選取省略號 (...)，然後選取 [刪除]。
7. 按一下 [檢閱 + 建立] 以檢閱為此原則選取的使用者群組。
8. 當您對指派所做的變更準備就緒之後，請選取 [儲存] 以儲存設定，並將原則部署到新的使用者集合。如果您在儲存設定之前選取 [取消]，則會捨棄對 [包含] 和 [排除] 索引標籤所做的所有變更。

變更原則設定

1. 在 [應用程式防護原則] 窗格中，選取您想要變更的原則。
2. 在 [Intune 應用程式保護] 窗格中，選取 [屬性]。
3. 在您要變更的設定對應的區段旁，選取 [編輯]。然後將設定變更為新的值。
4. 按一下 [檢閱 + 建立] 以檢閱此原則的更新設定。
5. 選取 [儲存] 以儲存您的變更。重複此程式來選取設定區域並修改，然後儲存您的變更，直到所有變更都完成為止。然後，您可以關閉 [Intune 應用程式保護 - 屬性] 窗格。

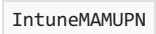
以裝置管理狀態為基礎的目標應用程式保護原則

在許多組織中，通常會允許終端使用者使用 Intune Mobile 裝置管理 (MDM) 受控裝置，例如公司擁有的裝置，以及僅使用 Intune 應用程式保護原則保護的未受管理裝置。非受控裝置通常稱為「攜帶您自己的裝置 (BYOD)」。

因為 Intune 應用程式保護原則是以身份識別為目標，所以使用者的保護設定可以套用至已註冊 (MDM 受控) 和未註冊的裝置，(沒有 MDM)。因此，您可以將 Intune 應用程式保護原則的目標設為 Intune 已註冊或取消註冊的 iOS/iPadOS 和 Android 裝置。您可以有一個非受控裝置的保護原則，其中有嚴格的資料外泄防護 (DLP) 控制項，以及 MDM 受控裝置的個別保護原則，其中 DLP 控制項可能會稍微寬鬆一點。如需如何在個人 Android Enterprise 裝置上運作的詳細資訊，請參閱[應用程式防護原則和工作設定檔](#)。

若要建立這些原則，請流覽至 Intune 主控台內的 [應用程式 > 應用程式防護 原則]，然後選取 [建立原則]。您也可以編輯現有的應用程式保護原則。若要讓應用程式保護原則同時套用至受控和未受管理的裝置，請流覽至 [應用程式] 頁面，並確認 [所有裝置類型上的應用程式 目標] 都設定為 [是]，這是預設值。如果您想要根據管理狀態細微指派，請將 [目標對所有裝置類型的應用程式] 設定為 [否]。

裝置類型

- **非受控**：針對 iOS/iPadOS 裝置，非受控裝置是 Intune MDM 管理或協力廠商 MDM/EMM 解決方案未傳遞  金鑰的任何裝置。針對 Android 裝置，非受控裝置是未偵測到 Intune MDM 管理的裝置。這包括由協力廠商 MDM 廠商管理的裝置。
- **Intune 受控裝置**：受控裝置是由 Intune MDM 管理。
- **Android 裝置系統管理員**：使用 Android 裝置 管理 API Intune 受管理的裝置。
- **Android Enterprise**：使用 Android Enterprise 工作設定檔或 Android Enterprise 完整裝置管理 Intune 受控裝

置。

在 Android 上，不論選擇哪種裝置類型，Android 裝置都會提示您安裝 Intune 公司入口網站應用程式。例如，如果您選取 [Android Enterprise]，則仍然會提示具有非受控 Android 裝置的使用者。

針對 iOS/iPadOS，若要強制將 [裝置類型] 選取專案強制執行至受管理的裝置 Intune，則需要額外的應用程式組態設定。這些設定會與 APP 服務通訊，以管理特定應用程式，且不會套用應用程式設定：

- 必須為所有 MDM 受控應用程式設定 IntuneMAMUPN。如需詳細資訊，請參閱[如何在 Microsoft Intune 中管理 iOS/iPadOS 應用程式之間的資料傳輸](#)。
- 必須為所有協力廠商和企業營運 MDM 受控應用程式設定 IntuneMAMDeviceID。IntuneMAMDeviceID 應該設定為裝置識別碼權杖。例如，`key=IntuneMAMDeviceID, value={{deviceID}}`。如需詳細資訊，請參閱[為受控 iOS/iPadOS 裝置新增應用程式設定原則](#)。
- 如果只設定 IntuneMAMDeviceID，Intune APP 會將裝置視為未受管理。

NOTE

如需以裝置管理狀態為基礎的應用程式保護原則的特定 iOS/iPadOS 支援資訊，請參閱 [以管理狀態為目標的 MAM 保護原則](#)。

原則設定

若要查看 iOS/iPadOS 和 Android 原則設定的完整清單，請選取下列其中一個連結：

- [iOS/iPadOS 原則](#)
- [Android 原則](#)

後續步驟

[監視合規性和使用者狀態](#)

另請參閱

- [適用於 Android 的 Managed 工作和學校應用程式](#)
- [當 iOS/iPadOS 應用程式受應用程式保護原則管理時，會發生什麼事](#)

Microsoft Intune 中的 Android 應用程式防護原則設定

2022/9/27 •

本文說明 Android 裝置的應用程式保護原則設定。您可以在入口網站的 [設定] 窗格 上，[針對應用程式保護原則設定](#)所描述的原則設定。原則設定有三種類別：資料保護設定、存取需求和條件式啟動。在本文中，[原則 管理的應用程式](#) 一詞是指使用應用程式保護原則設定的應用程式。

IMPORTANT

裝置上需要Intune 公司入口網站才能接收 Android 裝置的應用程式保護原則。

Intune Managed Browser已淘汰。針對受保護的Intune瀏覽器體驗使用[Microsoft Edge](#)。

資料保護

資料傳輸

“	“““	““
■■■■ Android ■■■■	選 ☐ 以防止此應用程式將公司或學校資料備份至 Android 備份服務。 選 ☐ 以允許此應用程式備份公司或學校資料。	Allow

[[	[[[[	[[[
████	選擇 [■] 以停用此應用程式中 [另存新檔] 選項的使用。如果您想要允許使用另存新檔, 請選擇 [■]*。當設定為 [封鎖] 時, 您可以設定 [允許使用者將複本儲存至選取的服務] 設定。 ■: Microsoft Excel、OneNote、PowerPoint 和 Word 都支援此設定。協力廠商和 LOB 應用程式可能也支援此功能。 - 只有當 [將 ██████████] 設定為 [受原則 ██████] 設定時, 才能設定此設定。 - 當 [將 ██████████] 設定設定為 [■] 時, 此設定會是 [允許]。 - 當 [將 ██████████] 設定設定為 [■] 時, 此設定會是「封鎖」且不允許的服務位置。	Allow
████████	使用者可以儲存至選取的服務 (商務用 OneDrive、SharePoint、相片媒體櫃、Box 和本機儲存體)。所有其他服務都會遭到封鎖。	■ 0 ■
████	一般而言, 當使用者在應用程式中選取超連結電話號碼時, 撥號應用程式將會開啟, 並預先填入電話號碼並準備好撥打電話。針對此設定, 選擇從受原則管理的應用程式起始時, 如何處理這種類型的內容傳輸: ■, ████████: 偵測到電話號碼時, 請勿傳輸通訊資料。 ██████: 允許特定撥號程式應用程式在偵測到電話號碼時起始連絡人。 ██████████: 允許任何受原則管理的撥號程式應用程式在偵測到電話號碼時起始連絡人。 ██████: 允許在偵測到電話號碼時, 使用任何撥號程式應用程式來起始連絡人。	████
████████	選取特定撥號程式應用程式時, 您必須提供 應用程式套件識別碼 。	Blank
████████	選取特定撥號程式應用程式時, 您必須提供撥號程式應用程式的名稱。	Blank

[[	[[[[	[[[
██████	指定哪些應用程式可以將資料傳輸至此應用程式： • █████: 只允許從其他受原則管理的應用程式進行傳輸。 • █████: 允許從任何應用程式傳輸資料。 • █: 不允許從任何應用程式傳輸資料, 包括其他受原則管理的應用程式。 有一些豁免應用程式和服務Intune允許資料傳輸。如需應用程式和服務的完整清單, 請參閱 資料傳輸豁免。	██████
██████	選 ☐ [█] 以停用 [開啟] 選項或其他選項, 以在此應用程式的帳戶之間共用資料。如果您想要允許使用 Open, 請選取 ☐*]。 當設定為 [█] 時, 您可以設定 [██████████], 以針對組織資料位置允許哪些服務。 █: 只有當 [██████████] 設定為 [受原則 █████] 設定時, 才能設定此設定。 • 當 [██████████] 設定設定為 [██████] 時, 此設定會是 [允許]。 • 當 [██████████] 設定設定為 [█] 時, 此設定會是「封鎖」, 且不允許服務位置。 • 下列應用程式支援此設定: - OneDrive 6.14.1 或更新版本。 - Android 版 Outlook 4.2039.2 或更新版本。 - Teams for Android 1416/1.0.0.2021173701 或更新版本。	Allow

ID	說明	類別
██████████	選取使用者可以從中開啟資料的應用程式儲存體服務。所有其他服務都會遭到封鎖。選取任何服務會防止使用者開啟資料。 支援的服務： • 商務用 OneDrive • SharePoint Online • 相機 • 相片媒體櫃 ■：相機不包含相片或相片庫存取。在 [Intune] 設定中選取 [庫] 時，您可以允許受管理的帳戶允許來自其裝置相片媒體櫃的 連入 資料傳入其受控應用程式。	██████████
██████████	指定何時可以搭配此應用程式使用剪下、複製和貼上動作。從下列專案中選擇： • ■：不允許在此應用程式與任何其他應用程式之間進行剪下、複製和貼上動作。 • ■：允許在此應用程式與其他受原則管理的應用程式之間進行剪下、複製和貼上動作。 • ■ 的原則：允許在此應用程式與其他受原則管理的應用程式之間進行剪下或複製。允許將來自任何應用程式的資料貼到此應用程式。 • ■：在此應用程式中剪下、複製和貼上沒有任何限制。	██████████
██████████	指定可從組織資料和帳戶剪下或複製的字元數。這將允許共用指定的字元數，否則會遭到 [限制與其他應用程式的剪下、複製和貼上] 設定封鎖。 預設值 = 0 ■：需要Intune 公司入口網站 5.0.4364.0 版或更新版本。	0
████ Google Assistant	選取 [■] 以封鎖螢幕擷取，並在使用此應用程式時封鎖 Google Assistant 存取裝置上的組織資料。選擇 [■] 也會在搭配公司或學校帳戶使用此應用程式時模糊應用程式切換器預覽映射。 ■：如果是無法存取組織資料的案例，使用者可以存取 Google Assistant。	■

☐☐	☐☐☐☐	☐☐☐
■	選 取 [需要], 然後為此原則指定核准的鍵盤清單。 未使用已核准鍵盤的使用者會收到下載並安裝已核准鍵盤的提示, 然後才可以使用受保護的應用程式。此設定需要應用程式具有 Intune SDK for Android 6.2.0 版或更新版本。	■
■	當您針對上一個選項選取 [需要] 時, 可以使用此選項。選擇 [選取] 以管理可與受此原則保護之應用程式搭配使用的鍵盤和輸入方法清單。您可以將其他鍵盤新增至清單, 並移除任何預設選項。您必須至少有一個核准的鍵盤才能儲存設定。經過一段時間後, Microsoft 可能會將其他鍵盤新增至新的應用程式保護原則清單, 這會要求系統管理員視需要檢閱和更新現有的原則。 若要新增鍵盤, 請指定: ■: 識別鍵盤的易記名稱, 使用者可以看見這個名稱。 ■ 符: Google Play 商店中應用程式的套件識別碼。例如, 如果 Play 商店中應用程式的 URL 是 <code>https://play.google.com/store/details?id=com.contoskeyboard.android.prod</code>, 則套件識別碼為 <code>com.contosokeyboard.android.prod</code>。此套件識別碼會以簡單的連結呈現給使用者, 以從 Google Play 下載鍵盤。 ■: 指派多個應用程式保護原則的使用者將只能使用所有原則通用的已核准鍵盤。	

加密

☐☐	☐☐☐☐	☐☐☐
■	選擇 [■] 以在此應用程式中啟用公司或學校資料的加密。Intune會使用一個 256 位的 256 位 AES 加密配置以及 Android 金鑰存放區系統, 安全地加密應用程式資料。資料會在檔案 I/O 工作期間同步加密。裝置儲存體上的內容一律會加密。新的檔案將會以 256 位金鑰加密。現有的 128 位加密檔案將會嘗試移轉至 256 位金鑰, 但不保證程式。使用 128 位金鑰加密的檔案仍可讀取。 加密方法已驗證 FIPS 140-2;如需詳細資訊, 請 參閱加密 FIPS 140-2 和 FIPS 140-3。	■

❏	❏❏❏	❏❏
■	指定組織帳戶的 OS 通知可共用多少組織資料。此原則設定會影響本機裝置和任何連線的裝置，例如穿戴式裝置和智慧型喇叭。應用程式可以提供額外的控制項來自訂通知行為，或選擇不接受所有值。從下列專案選取： ■: 不要共用通知。 - 如果應用程式不支援，則會允許通知。 ■: 不要在通知中共用組織資料。例如，「You have new mail」；「您有會議」。 - 如果應用程式不支援，將會封鎖通知。 ■: 在通知中共用組織資料 ■: 此設定需要應用程式支援： - Android 版 Outlook 4.0.95 或更新版本 - Teams for Android 1416/1.0.0.2020092202 或更新版本。	Allow

資料傳輸豁免

有一些豁免應用程式和平臺服務，Intune 應用程式保護原則允許資料來回傳輸。例如，Android 上所有 Intune 管理的應用程式都必須能夠在 Google 文字轉換語音中來回傳輸資料，才能大聲朗讀來自行動裝置畫面的文字。這份清單可能會有所變更，並反映被視為對安全生產力有用的服務和應用程式。

完整豁免

這些應用程式和服務完全允許 Intune 管理的應用程式來回傳輸資料。

❏❏❏/❏❏❏	❏
com.android.phone	原生手機應用程式
com.android.vending	Google Play 商店
com.android.documentsui	Android 檔選擇器
com.google.android.webview	WebView ，這是許多應用程式的必要專案，包括 Outlook。
com.android.webview	Webview ，這是許多應用程式的必要專案，包括 Outlook。
com.google.android.tts	Google 文字轉換語音
com.android.providers.settings	Android 系統設定
com.android.settings	Android 系統設定
com.azure.authenticator	Azure Authenticator 應用程式，這是在許多案例中成功驗證的必要專案。

包名稱	說明
com.microsoft.windowsintune.companyportal	Intune 公司入口網站

條件式豁免

在特定情況下，這些應用程式和服務只能從Intune管理的應用程式來回傳輸資料。

包名稱	應用程式/服務	說明
com.android.chrome	Google Chrome Browser	Chrome 用於 Android 7.0+ 上的某些 WebView 元件，而且永遠不會從檢視中隱藏。不過，從應用程式來回的資料流程一律會受到限制。
com.skype.complex	Skype	Skype 應用程式只允許用於導致撥打電話的特定動作。
com.android.providers.media	Android 媒體內容提供者	媒體內容提供者只允許用於鈴聲選取動作。
com.google.android.gms;com.google.android.gsf	Google Play 服務套件	Google 雲端通訊動作允許這些套件，例如推播通知。
com.google.android.apps.maps	Google Maps	允許位址進行導覽。

如需詳細資訊，請 [參閱應用程式的資料傳輸原則例外狀況](#)。

存取需求

需求	說明
要求 PIN	選擇 [] 以要求 PIN 才能使用此應用程式。第一次在公司或學校內容中執行應用程式時，系統會提示使用者設定此 PIN。 預設值 = 4 您可以使用 [PIN 以供存取] 區段下提供的設定來設定 PIN 強度。
PIN 長度	在存取已套用應用程式保護原則的應用程式之前，設定數值或密碼類型 PIN 的需求。數值需求只涉及數位，而密碼可以使用至少 1 個字母和至少 1 個特殊字元來定義。 預設值 = 8 值 ■：允許的特殊字元包括 Android 英文版鍵盤上的特殊字元和符號。

[[	]]]]
■ PIN	選 ☐ ☐ 以允許使用者使用簡單的 PIN 序列, 例如 <i>1234</i>、<i>1111</i>、<i>abcd</i> 或 <i>aaaa</i>。選 ☐ ☐ 以防止它們使用簡單的序列。簡單序列會在 3 個字元滑動視窗中核取。如果 ☐ Block, 則不會將 1235 或 1112 接受為使用者設定的 PIN, 但會允許 1122。 預設值 = ☐ ■: 如果已設定密碼類型 PIN, 且 [簡單 PIN] 設定為 [允許], 則使用者的 PIN 中至少需要一個字母 ☐ 至少一個特殊字元。如果已設定密碼類型 PIN, 且 [簡單 PIN] 設定為 [封鎖], 則使用者的 PIN 中至少需要一個數位 ☐ 一個字母, ☐ 至少一個特殊字元。
■ PIN ■■	指定 PIN 序列中的位數下限。 預設值 = 4
■■■, ■ PIN ■■	選 ☐ ☐ 以允許使用者使用生物特徵辨識來驗證 Android 裝置上的使用者。如果允許, 會使用生物特徵辨識來存取 Android 10 或更新版本裝置上的應用程式。
■■■ PIN ■■■■	若要使用此設定, 請選取 ☐ ☐, 然後設定閒置逾時。 預設值 = ☐
■ (■■■)	指定密碼或數值 (設定後的分鐘數,) PIN 會覆寫生物特徵辨識的使用。此逾時值應大於「在閒置」(分鐘後重新檢查存取需求)底下指定的值。 預設值 = 30
Android 9.0+ (■ 3 ■■■)	選 ☐ ☐ 要求使用者使用類別 3 生物識別技術登入。如需類別 3 生物特徵辨識的詳細資訊, 請參閱 Google 檔中的 生物特徵 辨識。
■■■■■ PIN ■■■ ■	選取 ☐ ☐ 以在偵測到生物特徵辨識變更時, 覆寫搭配 PIN 使用生物特徵辨識。 ■: 視 Android 裝置製造商而定, 並非所有形式的生物特徵辨識都支援密碼編譯作業。目前, 任何生物特徵辨識 (都支援密碼編譯作業, 例如, 裝置上的指紋、鳶尾花或臉部) 符合或超過 Android 檔中所定義之類別 3 生物特徵辨識的需求。請參 BIOMETRIC_STRONG 閱 BiometricManager.Authenticators.authenticate BiometricPrompt 類別的方法。您可能需要連絡裝置製造商, 以瞭解裝置特定的限制。
■■■ PIN	選取 ☐ ☐, 要求使用者在一段設定的一段時間之後, 以天為單位變更其應用程式 PIN。 當設定為 <i>[是]</i> 時, 您接著會設定需要 PIN 重設之前的天數。 預設值 = ☐

[[	[[[[
■	設定需要 PIN 重設之前的天數。 預設值 = 90
■■■ PIN ■	此設定會指定Intune將維護的先前 PIN 數目。任何新的 PIN 都必須與Intune維護的 PIN 不同。 預設值 = 0
■ PIN ■ PIN	選取 [■], 在已設定公司入口網站的已註冊裝置上偵測到裝置鎖定時停用應用程式 PIN。 預設值 = ■。
■■■■■	選擇 [■] 要求使用者使用其公司或學校帳戶登入, 而不是輸入 PIN 以存取應用程式。當設定為 [■], 且已開啟 PIN 或生物特徵辨識提示時, 會顯示公司認證和 PIN 或生物特徵辨識提示。 預設值 = ■
■ (■■■■■)	設定下列設定： ■: 這是重新檢查原則) 稍早定義 (存取需求之前的分鐘數。例如, 系統管理員在原則中開啟 PIN 和封鎖根目錄裝置、使用者開啟Intune管理的應用程式、必須輸入 PIN, 而且必須在非根目錄裝置上使用應用程式。使用此設定時, 使用者不需要輸入 PIN, 或在任何受Intune管理的應用程式上進行另一個根偵測檢查一段時間, 這一段時間就等於設定的值。 此原則設定格式支援正整數。 預設值 = 30 ■ ■: 在 Android 上, PIN 會與所有Intune管理的應用程式共用。當應用程式離開裝置的前景時, 會重設 PIN 計時器。使用者不需要在任何Intune管理的應用程式上輸入 PIN, 該應用程式會在此設定中定義的逾時期間內共用其 PIN 碼。

NOTE

若要深入瞭解同一組應用程式和使用者的存取一節中設定的多個Intune應用程式保護設定如何在 Android 上運作, 請[參閱在 Intune 中Intune MAM 常見問題](#)和[選擇性地使用應用程式保護原則存取動作來抹除資料](#)。

條件式啟動

設定條件式啟動設定, 以設定應用程式保護原則的登入安全性需求。

根據預設, 系統會提供數個設定與預先設定的值和動作。您可以刪除一些設定, 例如 *Min OS 版本*。您也可以從 [選取一個] 下拉式清單中選取其他設定。

[[	]]]]
PIN [REDACTED]	指定使用者在採取設定的動作之前，必須成功輸入 PIN 的嘗試次數。如果使用者在 PIN 嘗試次數上限之後無法成功輸入 PIN，使用者必須在成功登入其帳戶並完成 Multi-Factor Authentication (MFA) 挑戰之後重設其 PIN 碼。此原則設定格式支援正整數。<i>動作</i> 包括： ■ PIN - 使用者必須重設其 PIN。 [REDACTED] - 與應用程式相關聯的使用者帳戶會從裝置抹除。 預設值 = 5
[REDACTED]	MAM 應用程式可以離線執行的分鐘數。指定重新檢查應用程式存取需求之前) 分鐘 (的時間。<i>動作</i> 包括： [REDACTED] (■) - MAM 應用程式可離線執行的分鐘數。指定重新檢查應用程式存取需求之前) 分鐘 (的時間。在這段期間到期之後，應用程式需要向 Azure Active Directory (Azure AD) 進行使用者驗證，應用程式才能繼續執行。 此原則設定格式支援正整數。 預設值 = 720 分鐘 (12 小時)) ([REDACTED] - 在系統管理員) 定義這幾天 (離線執行之後，應用程式將要求使用者連線到網路並重新驗證。如果使用者成功驗證，他們可以繼續存取其資料，並重設離線間隔。如果使用者無法驗證，應用程式將會執行使用者帳戶和資料的選擇性抹除。如需詳細資訊，請參閱如何只抹除受控應用程式Intune公司資料。 此原則設定格式支援正整數。 預設值 = 90 ■ 此專案可能會出現多次，且每個實例都支援不同的動作。
[REDACTED]/Root [REDACTED]	此設定沒有要設定的值。<i>動作</i> 包括： [REDACTED] - 防止此應用程式在已越獄或 Root 破解的裝置上執行。使用者仍可繼續使用此應用程式進行個人工作，但必須使用不同的裝置來存取此應用程式中的工作或學校資料。 [REDACTED] - 與應用程式相關聯的使用者帳戶會從裝置抹除。
[REDACTED]	此設定沒有要設定的值。<i>動作</i> 包括： [REDACTED] - 當我們確認使用者已在 Azure Active Directory 中停用時，應用程式會封鎖對公司或學校資料的存取。 [REDACTED] - 當我們確認使用者已在 Azure Active Directory 中停用時，應用程式將會執行使用者帳戶和資料的選擇性抹除。

[[	]]]]
■ OS ■	指定使用此應用程式所需的最低 Android 作業系統。指定的 MIN OS ■■■■■ 將會觸發動作。<i>動作</i> 包括： ● ■ - 如果裝置上的 Android 版本不符合需求，使用者會看到通知。此通知可以關閉。 ● ■■ - 如果裝置上的 Android 版本不符合此需求，將會封鎖使用者存取。 ● ■■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 此原則設定格式支援 major.minor、major.minor.build、major.minor.build.revision。
OS ■■	指定使用此應用程式所需的 Android 作業系統上限。指定 ■ OS ■■■■■ 將會觸發動作。<i>動作</i> 包括： ● ■ - 如果裝置上的 Android 版本不符合需求，使用者會看到通知。此通知可以關閉。 ● ■■ - 如果裝置上的 Android 版本不符合此需求，將會封鎖使用者存取。 ● ■■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 此原則設定格式支援 major.minor、major.minor.build、major.minor.build.revision。
■■■■■	指定最低應用程式版本值的值。<i>動作</i> 包括： ● ■ - 如果裝置上的應用程式版本不符合需求，使用者會看到通知。此通知可以關閉。 ● ■■ - 如果裝置上的應用程式版本不符合需求，則會封鎖使用者存取。 ● ■■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 由於應用程式之間通常會有不同的版本控制配置，因此請建立一個以一個應用程式為目標之最低應用程式版本的原則 (例如，<i>Outlook 版本原則</i>)。 此專案可能會出現多次，且每個實例都支援不同的動作。 此原則設定格式支援 major.minor、major.minor.build、major.minor.build.revision。 此外，您可以設定終端使用者可在 ■ 取得企業營運 (LOB) 應用程式的更新版本。終端使用者會在 [■■■■■ 條件式啟動] 對話方塊中看到此資訊，這會提示終端使用者更新為最低版本的 LOB 應用程式。在 Android 上，此功能會使用公司入口網站。若要設定終端使用者應該更新 LOB 應用程式的位置，應用程式需要使用金鑰 傳送給它的受控應用程式設定原則。 com.microsoft.intune.myappstore 傳送的值會定義終端使用者將從哪個存放區下載應用程式。如果應用程式是透過公司入口網站部署，則值必須是 CompanyPortal。針對任何其他存放區，您必須輸入完整的 URL。

[[	[[[[
■■■	要求裝置具有 Google 發行的最低 Android 安全性修補程式。 ● ■ - 如果裝置上的 Android 版本不符合需求, 使用者會看到通知。此通知可以關閉。 ● ■■ - 如果裝置上的 Android 版本不符合此需求, 將會封鎖使用者存取。 ● ■■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 此原則設定支援 YYYY-MM-DD 的日期格式。
■■■ (■)	指定制造商 () 的分號分隔清單。這些值不區分大小寫。<i>動作</i> 包括: ● ■■ (■■■) - 只有符合指定製造商的裝置才能使用應用程式。所有其他裝置都會遭到封鎖。 ● ■■ (■■■) - 與應用程式相關聯的使用者帳戶會從裝置抹除。 如需使用此設定的詳細資訊, 請參閱 條件式啟動動作。
SafetyNet ■■	應用程式防護原則支援某些 Google Play 保護的 API。此設定特別會在使用者裝置上設定 Google 的 SafetyNet 證明, 以驗證這些裝置的完整性。指定 ■■ 或 ■■■■。 ■■■ 會告訴您裝置的一般完整性。具有竄改徵兆的根裝置、模擬器、虛擬裝置和裝置, 會失敗基本完整性。■■&■■■ 會告訴您裝置與 Google 服務的相容性。只有經過 Google 認證的未修改裝置才能通過這項檢查。 如果您在條件式啟動時選取 [SafetyNet ■■], 您可以指定使用硬體支援的金鑰作為評估類型。硬體支援的金鑰作為評估類型存在, 將表示裝置的完整性更高。如果裝置是以此設定為目標, 則 MAM 原則會封鎖不支援硬體支援金鑰的裝置。硬體支援的金鑰提供更強固的根偵測, 以回應較新類型的根目錄工具和方法, 這些工具和方法永遠無法由軟體專用解決方案可靠地偵測。在 APP 中, 一旦設定 SafetyNet ■ 證明, 就會將 [■■ SafetyNet ■■] 設定為 [■■■], 以啟用硬體證明。硬體支援的證明會利用隨附于 Android 8.1 和更新版本所安裝裝置的硬體型元件。從舊版 Android 升級至 Android 8.1 的裝置不太可能有硬體支援證明所需的硬體型元件。雖然從 Android 8.1 隨附的裝置開始應該廣泛支援此設定, 但 Microsoft 強烈建議您在廣泛啟用此原則設定之前, 先個別測試裝置。 ■: 不支援此評估類型的裝置將會根據 SafetyNet 裝置證明動作進行封鎖或抹除。想要使用這項功能的組織必須確保使用者有支援的裝置。如需 Google 建議裝置的詳細資訊, 請參閱 Android Enterprise 建議需求。 <i>動作</i> 包括: ● ■ - 如果裝置不符合 Google 的 SafetyNet 證明掃描, 使用者會根據設定的值看到通知。此通知可以關閉。 ● ■■ - 如果裝置不符合 Google 的 SafetyNet 證明掃描, 則會根據設定的值封鎖使用者存取。 ● ■■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 如需與此設定相關的常見問題, 請參閱 MAM 和應用程式保護的常見問題。

[[	]]]]
■■■■■	應用程式防護原則支援某些 Google Play 保護的 API。此設定特別可確保已針對終端使用者裝置開啟 Google 的驗證應用程式掃描。如果設定，使用者將會遭到封鎖而無法存取，直到他們在其 Android 裝置上開啟 Google 的應用程式掃描為止。 動作 包括： ● ■ - 如果未開啟 Google 在裝置上的驗證應用程式掃描，使用者會看到通知。此通知可以關閉。 ● ■■ - 如果未開啟 Google 在裝置上的驗證應用程式掃描，使用者會遭到封鎖而無法存取。 Google 驗證應用程式掃描的結果會顯示在主控台中 ■■■■■ 報告中。
■■■■■	藉由使用 Min ■■■■■，您可以指定在終端使用者裝置上強制執行之公司入口網站的特定最小定義版本。此條件式啟動設定可讓您在不符合每個值時，將值設定為 [■■■]、[■■■] 和 [■] 作為可能的動作。此值的可能格式會遵循 模式 [Major].[Minor]、[Major].[次要]。[Build]，或 [Major].[次要]。[組建]。[修訂]。假設某些終端使用者可能不偏好現場強制更新應用程式，在設定此設定時，[警告] 選項可能很理想。Google Play 商店在只傳送應用程式更新的差異位元組方面有不少的效能，但如果使用者在更新時正在處理資料，這仍然可以是大量使用者可能不想要利用的資料。強制更新，因而下載更新的應用程式，可能會在更新時產生非預期的資料費用。如需詳細資訊，請參閱 Android 原則設定。
■■■ (n) ■■■■	您可以將 Android 裝置的公司入口網站 (CP) 版本的存留期設定為天數上限。此設定可確保使用者在) 天數內 (特定範圍的 CP 版本。值必須介於 0 到 365 天之間。當不符合裝置的設定時，會觸發此設定的動作。動作包括 ■■、■■ 或 ■。如需相關資訊，請參閱 Android 原則設定。
■■■■■	應用程式防護原則可以利用 Intune-MTD 連接器。指定可接受使用此應用程式的最大威脅層級。威脅取決於您在終端使用者裝置上選擇的 Mobile Threat Defense (MTD) 廠商應用程式。指定 [安全]、[低]、[中] 或 [高]。受保護不需要裝置上的威脅，而且是最嚴格的可設定值，而 High 基本上需要使用中 Intune對 MTD 連線。動作 包括： ● ■■ - 如果您在終端使用者裝置上選擇的 Mobile Threat Defense (MTD) 廠商應用程式所決定的威脅層級不符合此需求，則會封鎖使用者存取。 ● ■■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 如需使用此設定的詳細資訊，請參閱在未註冊裝置的Intune中啟用 Mobile Threat Defense 連接器。

[[	]]]]
	此設定會決定 Android 裝置是否有符合最低密碼需求的裝置 PIN。如果裝置鎖定不符合最低密碼需求，應用程式防護原則可以採取動作。 ■ 包括： ● ■ ● ■ ● ■ 此複雜度值是以 Android 11+ 為目標。對於在 Android 10 和更早版本上運作的裝置，將複雜度值設定為低、中或高會預設為 ■ 的預期行為。如需詳細資訊，請參閱 Google 的開發人員檔 getPasswordComplexity、PASSWORD_COMPLEXITY_LOW、PASSWORD_COMPLEXITY_MEDIUM和 PASSWORD_COMPLEXITY_HIGH。 ■ 包括： ● ■ - 如果裝置鎖定不符合最低密碼需求，使用者會看到通知。可以關閉通知。 ● ■ - 如果裝置鎖定不符合最低密碼需求，將會封鎖使用者存取。 ● ■ - 如果裝置鎖定不符合最低密碼需求，則會從裝置抹除與應用程式相關聯的使用者帳戶。

iOS 應用程式防護原則設定

2022/9/27 •

本文說明 iOS/iPadOS 裝置的應用程式保護原則設定。當您建立新原則時，[可以在入口網站的 \[設定\] 窗格](#) 上設定應用程式保護原則所描述的原則設定。

原則設定有三種類別：[資料重新配置](#)、[存取需求](#) 和 [條件式啟動](#)。在本文中，原則 [管理的應用程式](#) 一詞是指使用應用程式保護原則設定的應用程式。

IMPORTANT

Intune Managed Browser已淘汰。針對受保護的Intune瀏覽器體驗使用[Microsoft Edge](#)。

資料保護

資料傳輸

II	IIII	III
■■■■ iTunes ■ iCloud ■	選 ■ [■] 以防止此應用程式將公司或學校資料備份至 iTunes 和 iCloud。選 ■ [■] 以允許此應用程式將公司或學校資料備份至 iTunes 和 iCloud。	Allow
■■■■■	指定哪些應用程式可以從此應用程式接收資料： ● ■■■■: 允許傳送至任何應用程式。接收應用程式將能夠讀取和編輯資料。 ● ■: 不允許將資料傳輸至任何應用程式，包括其他受原則管理的應用程式。如果使用者執行 Managed Open-in 函式並傳輸檔，資料將會加密且無法讀取。 ● ■■■■■: 只允許傳送至其他受原則管理的應用程式。 ■: 使用者可以透過開啟或共用擴充功能，將內容傳輸至未註冊裝置上的 Unmanaged 應用程式，或允許共用至 Unmanaged 應用程式的已註冊裝置。傳輸的資料會由Intune加密，而非受控應用程式無法讀取。 ● ■ OS ■■■■■: 只允許將資料傳輸至其他受原則管理的應用程式，以及將檔案傳輸至已註冊裝置上的其他 MDM 受控應用程式。 ■: ■ OS ■■■■■ 僅適用於已註冊 MDM 的裝置。如果此設定是以未註冊裝置上的使用者為目標，則會套用受 ■■■■■ 值的行為。假設傳送	■■■■■

☐☐	☐☐☐☐ 的應用程式已設定 IntuneMAMUPN 和 IntuneMAMOID, 使用者將能夠透過 [開啟] 或 [共用擴充功能] 將未加密的內容傳輸到 iOS MDM	☐☐☐
	allowOpenFromManagedtoUnmanaged 設定所允許的任何應用程式;如需詳細資訊, 請參閱如何在 Microsoft Intune 中管理 iOS 應用程式之間的資料傳輸。如需此 iOS/iPadOS MDM 設定的詳細資訊, 請參閱 https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf。 ● ☐☐/☐☐ 的原則受控應用程式: 只允許傳送至其他受原則管理的應用程式, 並篩選 OS [開啟/共用] 對話方塊, 只顯示受原則管理的應用程式。若要設定 [☐☐/☐☐] 對話方塊的篩選, 應用程式 () 做為檔案/檔來源, 以及應用程式 (可開啟此檔案/檔的), 才能擁有適用於 iOS 的 Intune SDK 8.1.1 版或更新版本。 ■: 如果應用程式支援 Intune 私有資料類型, 則使用者可以透過 [開啟] 或 [共用] 延伸模組將內容傳輸至 Unmanaged 應用程式。傳輸的資料會由 Intune 加密, 而非受控應用程式無法讀取。 此外, 當設定為 [☐☐☐☐] 或 [☐☐] 時, 焦點搜尋 (可讓您在應用程式內搜尋資料,) 並封鎖 Siri 快捷方式 iOS 功能。 此原則也可以套用至 iOS/iPadOS 通用連結。一般 Web 連結是由 [在原則 ☐☐☐☐] Intune Managed Browser 管理。 有一些豁免應用程式和服務, Intune 預設可能會允許資料傳輸。此外, 如果您需要允許資料傳輸至不支援應用程式 Intune 應用程式, 您可以建立自己的豁免。如需詳細資訊, 請參閱 資料傳輸豁免。	
☐☐☐☐☐☐	當您針對上一個選項選取受 <i>原則管理的應用程式</i> 時, 可以使用此選項。	

[[	[[[[	[[[
■■■■■	指定哪些 iOS/iPadOS 通用連結 應在指定的 <i>Unmanaged</i> 應用程式中開啟，而不是由 [■■■■■ Web ■■■] 設定所指定的受保護瀏覽器。您必須連絡應用程式開發人員，以判斷每個應用程式的正確通用連結格式。	
■ Managed ■■■	指定哪些 iOS/iPadOS 通用連結 應 在指定的受控應用程式中開啟，而不是由 [■■■■■ Web ■■■] 設定所指定的受保護瀏覽器。您必須連絡應用程式開發人員，以判斷每個應用程式的正確通用連結格式。	
■■■■■	選擇 [■] 以停用此應用程式中 [另存新檔] 選項的使用。如果您想要允許使用另存新檔，請選擇 [■]*。當設定為 [封鎖] 時，您可以設定 [允許使用者將複本儲存至選取的服務] 設定。 ■： Microsoft Excel、OneNote、Outlook、PowerPoint 和 Word 都支援此設定。協力廠商和 LOB - 應用程式也可以支援它。 只有當 [將 ■■■■■■■■■■] 設定為 [受原則 ■■■■■]、[具有 OS ■■■■■■■■■■] 或 [使用 ■■■/■■■■ 原則管理的應用程式] 設定時，才能設定此設定。 - 當 [將 ■■■■■■■■■■] 設定設定為 [■■■■■] 時，此設定會是 [允許]。 - 當 [將 ■■■■■■■■■■] 設定設定為 [■] 時，此設定會是「封鎖」且不允許的服務位置。	Allow
■■■■■■■■■■	使用者可以儲存至選取的服務 (商務用 OneDrive、SharePoint、相片媒體櫃和本機儲存體)。所有其他服務都會遭到封鎖。商務用 OneDrive: 您可以將檔案儲存至 商務用 OneDrive 和 SharePoint Online。SharePoint: 您可以將檔案儲存至內部部署 SharePoint。相片媒體櫃: 您可以在本機將檔案儲存至相片庫。本機儲存體: Managed 應用程式可以在本機儲存組織資料的複本。這不包括將檔案儲存到本機非受控位置，例如裝置上的檔案應用程式。	■ 0 ■

[[	[[[[	[[[
■■■■■	一般而言，當使用者在應用程式中選取超連結電話號碼時，撥號應用程式將會開啟，並預先填入電話號碼並準備好撥打電話。針對此設定，選擇從受原則管理的應用程式起始時，如何處理這種類型的內容傳輸： ■, ■■■■■: 偵測到電話號碼時，請勿傳輸通訊資料。 ■■■■■: 允許特定撥號程式應用程式在偵測到電話號碼時起始連絡人。 ■■■■■: 允許在偵測到電話號碼時，使用任何撥號程式應用程式來起始連絡人。 ■: 此設定需要Intune SDK 12.7.0 和更新版本。如果您的應用程式依賴撥號程式功能，但未使用正確的Intune SDK 版本，請考慮新增「tel;telprompt」作為資料傳輸豁免。一旦應用程式支援正確的Intune SDK 版本，就可以移除豁免。	■■■■■
■■■■■ URL ■■■■	選取特定撥號程式應用程式時，您必須提供用來在 iOS 裝置上啟動撥號程式應用程式的撥號程式應用程式 URL 配置。如需詳細資訊，請參閱 Apple 的 Phone Links 相關檔。	Blank
■■■■■	指定哪些應用程式可以將資料傳輸至此應用程式： ■■■■■: 允許從任何應用程式傳輸資料。 ■: 不允許從任何應用程式傳輸資料，包括其他受原則管理的應用程式。 ■■■■■: 只允許從其他受原則管理的應用程式進行傳輸。 ■■■■■: 允許從任何應用程式傳輸資料。將所有沒有使用者身分識別的傳入資料視為您組織的資料。資料會以設定所 <code>IntuneMAMUPN</code> 定義的 MDM 已註冊使用者身分識別標示。 ■: ~~xxxxxxxxxxxx~~ 僅適用於已註冊 MDM 的裝置。如果此設定是以未註冊裝置上的使用者為目標，則會套用 [~~xxxxxx~~] 值的行為。 如果將此設定設定為 [■] 或 [受原則管理的應用程式]，啟用多重身分識別 MAM 的 ■■■■ 會在接收 Unmanaged 資料時嘗試切換至 Unmanaged 帳戶。如果沒有登入應用程式的 Unmanaged 帳戶，或應用程式無法切換，則會封鎖傳入資料。	■■■■■

CC	CCCC	CCC

■■■■■	選 ■ [■] 以停用 [開啟] 選項或其他選項, 以在此應用程式的帳戶之間共用資料。如果您想要允許使用 Open, 請選取 [■*]*。 當設定為 [■] 時, 您可以設定 [■■■■■ ■■■], 以針對組織資料位置允許哪些服務。 ■: - 只有當 [■■■■■■■■■■] 設定為 [受原則 ■■■■■] 設定時, 才能設定此設定。 - 當 [■■■■■■■■■■] 設定設為 [■■■■■] 或 [■■■■■■■■■■] 設定時, 此設定會是 [允許]。 - 當 [■■■■■■■■■■] 設定設為 [■] 時, 此設定會是「封鎖」, 且不允許服務位置。 - 下列應用程式支援此設定: - OneDrive 11.45.3 或更新版本。 - iOS 版 Outlook 4.60.0 或更新版本。 - 適用於 iOS 3.17.0 或更新版本的 Teams。	Allow

[[	]]]]	]]
■■■■■	選取使用者可以從中開啟資料的應用程式儲存體服務。所有其他服務都會遭到封鎖。選取任何服務會防止使用者從外部位置開啟資料。 支援的服務： ● 商務用 OneDrive ● SharePoint Online ● 相機 ● 相片媒體櫃 ■：相機不包含相片或相片庫存取。在 [■■■■Intune■■■■] 設定中選取 [■ 庫] 時，您可以允許受管理的帳戶允許來自其裝置相片媒體櫃的 連入 資料傳入其受控應用程式。	■■■
■■■■■	指定何時可以搭配此應用程式使用剪下、複製和貼上動作。從下列專案選取： ● ■■：不允許在此應用程式與任何其他應用程式之間進行剪下、複製和貼上動作。 ● ■■■■■：允許在此應用程式與其他受原則管理的應用程式之間進行剪下、複製和貼上動作。 ● ■■■■■ 的原則：允許在此應用程式與其他受原則管理的應用程式之間進行剪下或複製。允許將來自任何應用程式的資料貼到此應用程式。 ● ■■■■：在此應用程式中剪下、複製和貼上沒有任何限制。	■■■
■■■■■	指定可從組織資料和帳戶剪下或複製的字元數。無論 [■■■■■■■■■■ 上] 設定為何，這都允許將指定數目的字元共用到任何應用程式。 預設值 = 0 ■：應用程式必須Intune SDK 9.0.14 版或更新版本。	0

☐	☐☐☐	☐☐☐
■	選擇 [■] 以防止在受控應用程式中使用協力廠商鍵盤。 啟用此設定時，使用者會收到一次性訊息，指出已封鎖使用協力廠商鍵盤。當使用者第一次與需要使用鍵盤的組織資料互動時，就會出現此訊息。使用受控應用程式時，只有標準 iOS/iPadOS 鍵盤可供使用，而且所有其他鍵盤選項都會停用。此設定會影響多重身分識別應用程式的組織和個人帳戶。此設定不會影響在 Unmanaged 應用程式中使用協力廠商鍵盤。 ■：此功能需要應用程式使用 Intune SDK 12.0.16 版或更新版本。SDK 版本從 8.0.14 到 12.0.15 的應用程式將無法正確地套用至多重身分識別應用程式。如需詳細資訊，請 參閱已知問題：iOS/iPadOS 中不會針對個人帳戶封鎖協力廠商鍵盤。	Allow

NOTE

受控裝置的 IntuneMAMUPN 需要應用程式保護原則。這適用於需要已註冊裝置的任何設定。

加密

☐	☐☐☐	☐☐☐
■	選擇 [需要] 以在此應用程式中啟用公司或學校資料的加密。Intune 會強制 iOS/iPadOS 裝置層級加密，以保護裝置鎖定時的應用程式資料。此外，應用程式可以選擇性地使用 Intune APP SDK 加密來加密應用程式資料。Intune APP SDK 會使用 iOS/iPadOS 密碼編譯方法，將 256 位 AES 加密套用於應用程式資料。 當您啟用此設定時，使用者可能需要設定並使用裝置 PIN 來存取其裝置。如果沒有裝置 PIN，而且需要加密，系統會提示使用者設定 PIN，並顯示「您的組織要求您先啟用裝置 PIN 以存取此應用程式」訊息。 移至 官方 Apple 檔，以查看哪些 iOS/iPadOS 加密模組已通過 FIPS 140-2 驗證。	■

功能

☐	☐☐☐	☐☐☐

☐☐	☐☐☐☐	☐☐☐
	選擇 [封鎖] 以防止受原則管理的應用程式將資料儲存到裝置的原生應用程式，(連絡人、行事曆和小工具)，並防止在受原則管理的應用程式內使用增益集。應用程式可能會提供額外的控制項，以自訂特定原生應用程式的資料同步處理行為，或不接受此控制項。 如果您選擇 [允許]，受原則管理的應用程式可以在受原則管理的應用程式內支援並啟用這些功能時，將資料儲存至原生應用程式或使用增益集。 當您執行選擇性抹除以從應用程式移除工作或學校資料時，會移除直接從應用程式同步至原生連絡人應用程式的連絡人資料。無法抹除從原生連絡人應用程式同步至另一個外部來源的任何連絡人資料。目前，這僅適用於 iOS 版 Outlook 應用程式；如需詳細資訊，請 參閱部署 iOS 版 Outlook 和 Android 應用程式組態設定。 ■：下列應用程式支援這項功能： • <i>iOS 版 Outlook</i>	Allow
	選 ■ [■] 以防止應用程式列印公司或學校資料。如果您將此設定保留為預設值 Allow，則使用者將能夠匯出和列印所有組織資料。	Allow

☐	☐☐☐	☐☐☐
	輸入 單一 Unmanaged 瀏覽器的通訊協定。從受原則管理應用程式) (HTTP/HTTPS 連結的 Web 內容, 將會在支援此通訊協定的任何應用程式中開啟。Web 內容將會在目標瀏覽器中非受控。 只有當您想要與未使用Intune應用程式保護原則啟用的特定瀏覽器共用受保護的內容時, 才應該使用此功能。您必須連絡瀏覽器廠商, 以判斷所需的瀏覽器所支援的通訊協定。 ■: 只包含通訊協定前置詞。如果您的瀏覽器需要表單 <code>mybrowser://www.microsoft.com</code> 的連結, 請輸入 <code>mybrowser</code>。 連結會轉譯為: <code>http://www.microsoft.com</code> > <code>mybrowser://www.microsoft.com</code> <code>https://www.microsoft.com</code> > <code>mybrowsers://www.microsoft.com</code>	Blank
	指定如何透過組織帳戶的 OS 通知來共用組織資料。此原則設定會影響本機裝置和任何連線的裝置, 例如穿戴式裝置和智慧型喇叭。應用程式可以提供額外的控制項來自訂通知行為, 或選擇不接受所有值。從下列專案選取: ☐: 不要共用通知。 - 如果應用程式不支援, 則會允許通知。 ☐☐☐: 例如, 不要在通知中共用組織資料。 「您有新郵件」;「您有會議」。 - 如果應用程式不支援, 則會允許通知。 ■: 在通知中共用組織資料。 ■: 此設定需要應用程式支援: - iOS 版 Outlook 4.34.0 或更新版本 - 的 iOS 2.0.22 版或更新版本 Teams。	Allow

NOTE

沒有任何資料保護設定可控制 iOS/iPadOS 裝置上的 Apple 受控開啟功能。若要使用管理 Apple Open-in, 請參閱[使用 Microsoft Intune 管理 iOS/iPadOS 應用程式之間的資料傳輸](#)。

資料傳輸豁免

有些豁免應用程式和平臺服務Intune應用程式保護原則可能會允許在某些情況下來回傳輸資料。這份清單可能

會有所變更，並反映被視為對安全生產力有用的服務和應用程式。

協力廠商非受控應用程式可以新增至允許資料傳輸例外狀況的豁免清單。如需其他詳細資料和範例，請參閱[如何建立Intune應用程式保護原則 \(APP\) 資料傳輸原則的例外狀況](#)。豁免 Unmanaged 應用程式必須根據 iOS URL 通訊協定叫用。例如，針對 Unmanaged 應用程式新增資料傳輸豁免時，如果受到原則限制，仍會防止使用者進行剪下、複製和貼上作業。這種豁免類型仍然會防止使用者在受控應用程式內使用「開啟」動作來共用或儲存資料，以免應用程式，因為它不是以 iOS URL 通訊協定為基礎。如需 Open-in 的詳細資訊，請參閱[搭配 iOS 應用程式使用應用程式保護](#)。

URL 格式 (URL)	名稱
<code>skype</code>	Skype
<code>app-settings</code>	裝置設定
<code>itms; itmss; itms-apps; itms-appss; itms-services</code>	App Store
<code>calshow</code>	原生行事曆

IMPORTANT

在 2020 年 6 月 15 日之前建立的應用程式保護原則包含 *tel* 和 *telprompt* URL 配置，作為預設資料傳輸豁免的一部分。這些 URL 配置可讓 Managed 應用程式起始撥號程式。應用程式保護原則設定 [[限制使用其他應用程式進行 Web 內容傳輸](#)] 已取代此功能。如果起始撥號程式功能的受控應用程式包含 Intune SDK 12.7.0 或更新版本，系統管理員應該從資料傳輸豁免中移除 *tel;telprompt*，並依賴應用程式保護原則設定。

IMPORTANT

在 Intune SDK 14.5.0 或更新版本中，在資料傳輸豁免中包含 *sms* 和 *mailto* URL 配置，也可讓您將組織資料共用至受原則管理應用程式內之 *sms* 的 MFMessageCompose (，以及適用於 *mailto* 檢視控制器的 MFMailCompose (。

通用連結

通用連結可讓使用者直接啟動與連結相關聯的應用程式，而不是由 [[限制使用其他應用程式進行 Web 內容傳輸](#)] 設定所指定的受保護瀏覽器。您必須連絡應用程式開發人員，以判斷每個應用程式的正確通用連結格式。

豁免通用連結

藉由將通用連結新增至 *Unmanaged* 應用程式，您可以啟動指定的應用程式。若要新增應用程式，您必須將連結新增至豁免清單。

Caution

這些通用連結的目標應用程式是非受控的，而新增豁免可能會導致資料安全性流失。

預設應用程式通用連結豁免如下：

URL 格式 (URL)	名稱
<code>http://maps.apple.com;</code> <code>https://maps.apple.com</code>	地圖應用程式
<code>http://facetime.apple.com;</code> <code>https://facetime.apple.com</code>	FaceTime App

如果您不想要允許預設的通用連結豁免，您可以將其刪除。您也可以為協力廠商或 LOB 應用程式新增通用連

結。豁免的通用連結允許萬用字元，例如 `http://*.sharepoint-df.com/*` 。

Managed 通用連結

藉由將通用連結新增至 受控 應用程式，您可以安全地啟動指定的應用程式。若要新增應用程式，您必須將連結新增至 Managed 清單。如果目標應用程式已套用應用程式保護原則，選取連結將會啟動應用程式。如果目標應用程式未套用應用程式保護原則，選取連結將會啟動受保護的瀏覽器。

預設的受控通用連結如下：

MANAGED APP 通用連結	受控通用連結
<code>http://*.onedrive.com/*;</code> <code>https://*.onedrive.com/*;</code>	OneDrive
<code>http://*.appsplatform.us/*;</code> <code>http://*.powerapps.cn/*;</code> <code>http://*.powerapps.com/*;</code> <code>http://*.powerapps.us/*;</code> <code>https://*.powerbi.com/*;</code> <code>https://app.powerbi.cn/*;</code> <code>https://app.powerbigov.us/*;</code> <code>https://app.powerbi.de/*;</code>	PowerApps
<code>http://*.powerbi.com/*;</code> <code>http://app.powerbi.cn/*;</code> <code>http://app.powerbigov.us/*;</code> <code>http://app.powerbi.de/*;</code> <code>https://*.appsplatform.us/*;</code> <code>https://*.powerapps.cn/*;</code> <code>https://*.powerapps.com/*;</code> <code>https://*.powerapps.us/*;</code>	Power BI
<code>http://*.service-now.com/*;</code> <code>https://*.service-now.com/*;</code>	ServiceNow
<code>http://*.sharepoint.com/*;</code> <code>http://*.sharepoint-df.com/*;</code> <code>https://*.sharepoint.com/*;</code> <code>https://*.sharepoint-df.com/*;</code>	SharePoint
<code>http://web.microsoftstream.com/video/*;</code> <code>http://msit.microsoftstream.com/video/*;</code> <code>https://web.microsoftstream.com/video/*;</code> <code>https://msit.microsoftstream.com/video/*;</code>	Stream
<code>http://*teams.microsoft.com/l/*;</code> <code>http://*devspaces.skype.com/l/*;</code> <code>http://*teams.live.com/l/*;</code> <code>http://*collab.apps.mil/l/*;</code> <code>http://*teams.microsoft.us/l/*;</code> <code>http://*teams-fl.microsoft.com/l/*;</code> <code>https://*teams.microsoft.com/l/*;</code> <code>https://*devspaces.skype.com/l/*;</code> <code>https://*teams.live.com/l/*;</code> <code>https://*collab.apps.mil/l/*;</code> <code>https://*teams.microsoft.us/l/*;</code> <code>https://*teams-fl.microsoft.com/l/*;</code>	Teams

MANAGED APP 名稱	說明
http://tasks.office.com/*; https://tasks.office.com/*; http://to-do.microsoft.com/sharing*; https://to-do.microsoft.com/sharing*;	Todo
http://*.yammer.com/*; https://*.yammer.com/*;	Yammer
http://*.zoom.us/*; https://*.zoom.us/*;	縮放

如果您不想要允許預設的 Managed 通用連結，您可以將它們刪除。您也可以為協力廠商或 LOB 應用程式新增通用連結。

存取需求

名稱	說明	預設值
■ PIN	選 ☐ [■] 以要求 PIN 才能使用此應用程式。第一次在公司或學校內容中執行應用程式時，系統會提示使用者設定此 PIN。在線上或離線工作時，會套用 PIN。 您可以使用 [PIN 以供存取] 區段下提供的設定來設定 PIN 強度。	☐
PIN ☐	在存取已套用應用程式保護原則的應用程式之前，設定數值或密碼類型 PIN 的需求。數值需求只涉及數位，而密碼可以使用至少 1 個字母 ☐ 至少 1 個特殊字元來定義。 **注意:** 若要設定密碼類型，應用程式必須 Intune SDK 7.1.12 版或更新版本。數值型別沒有 Intune SDK 版本限制。允許的特殊字元包括 iOS/iPadOS 英文版鍵盤上的特殊字元和符號。	☐
☐ PIN	選 ☐ [■] 以允許使用者使用簡單的 PIN 序列，例如 1234、1111、abcd 或 aaaa。選取 ☐ [■] 以防止它們使用簡單的序列。簡單序列會在 3 個字元滑動視窗中核取。如果 ☐ Block，則不會將 1235 或 1112 接受為使用者設定的 PIN，但會允許 1122。 ■: 如果已設定密碼類型 PIN，且 [允許簡單 PIN] 設定為 [是]，則使用者的 PIN 中至少需要 1 個字母 ☐ 至少 1 個特殊字元。如果已設定密碼類型 PIN，且 [允許簡單 PIN] 設定為 [否]，則使用者的 PIN 中至少需要 1 個數字 ☐ 1 個字母，☐ ☐ 至少 1 個特殊字元。	Allow
☐ PIN ☐	指定 PIN 序列中的位數下限。	4

[[	[[[[	[[[[
■ iOS 8+) ■■■, ■ PIN (	選 ■ [■] 以允許使用者使用 Touch ID , 而不是 PIN 來存取應用程式。	Allow
■■ PIN ■■■	若要使用此設定, 請選取 [■], 然後設定閒置逾時。	■
■ (■■■)	指定密碼或數位 (設定的分鐘數,) PIN 會覆寫指紋或臉部作為存取方法的使用。此逾時值應大於「在閒置」(分鐘後重新檢查存取需求」底下指定的值。	30
■ iOS 11+ (■■■, ■ PIN)	選 ■ [■] 以允許使用者使用臉部辨識技術來驗證 iOS/iPadOS 裝置上的使用者。如果允許, 則必須使用臉部識別碼來存取具備臉部識別碼的裝置上的應用程式。	Allow
■■■ PIN	選取 [■], 要求使用者在一段設定的一段時間之後, 以天為單位變更其應用程式 PIN。 當設定為 <i>[是]</i> 時, 您接著會設定需要 PIN 重設之前的天數。	■
■	設定需要 PIN 重設之前的天數。	90
■■ PIN ■■■ PIN	選 ■ [■], 以在已設定公司入口網站的已註冊裝置上偵測到裝置鎖定時停用應用程式 PIN。 <i>**注意:** 應用程式必須 Intune SDK 7.0.1 版或更新版本。必須設定 IntuneMAMUPN 設定, 應用程式才能偵測註冊狀態。</i> 在 iOS/iPadOS 裝置上, 您可以讓使用者使用 觸控標識 符或 臉部標識 符來證明其身分識別, 而不是 PIN。Intune 使用 LocalAuthentication API 來驗證使用 Touch ID 和臉部識別碼的使用者。若要深入瞭解觸控識別碼和臉部識別碼, 請參閱 iOS 安全性指南 。 當使用者嘗試使用此應用程式搭配其公司或學校帳戶時, 系統會提示他們提供指紋身分識別或臉部身分識別, 而不是輸入 PIN。啟用此設定時, 使用公司或學校帳戶時, 應用程式切換器預覽映射將會模糊。如果裝置的生物特徵辨識資料庫有任何變更, Intune 會在符合下一個閒置逾時值時提示使用者輸入 PIN。生物特徵辨識資料的變更包括新增或移除指紋或臉部以進行驗證。如果 Intune 使用者沒有 PIN 集, 系統會引導他們設定 Intune PIN。	Enable

[[	[[[[	[[[[
■■■■■	選 [■] 要求使用者使用其公司或學校帳戶登入, 而不是輸入 PIN 以存取應用程式。如果您將此設定為 [■], 且已開啟 PIN 或生物特徵辨識提示, 則會顯示公司認證和 PIN 或生物特徵辨識提示。	■
■ (■■■■■)	設定在應用程式要求使用者再次指定存取需求之前, 必須通過的閒置分鐘數。 例如, 系統管理員在原則中開啟 PIN 和封鎖根目錄裝置、使用者開啟Intune管理的應用程式、必須輸入 PIN, 而且必須在非根目錄裝置上使用應用程式。使用此設定時, 使用者不需要輸入 PIN, 或在任何受Intune管理的應用程式上進行另一個根偵測檢查, 一段時間就等於設定的值。 **注意:** 在 iOS/iPadOS 上, PIN 會在 ■ 者的所有受Intune管理應用程式之間共用。當應用程式離開裝置的前景時, 會重設特定 PIN 的 PIN 計時器。使用者不需要在任何Intune管理的應用程式上輸入 PIN, 該應用程式會在此設定中定義的逾時期間內共用其 PIN 碼。此原則設定格式支援正整數。	30

NOTE

若要深入瞭解同一組應用程式和使用者的存取一節中設定的多個Intune應用程式保護設定如何在 iOS/iPadOS 上運作, 請參閱Intune MAM 常見問題, 以及在Intune中使用應用程式保護原則存取動作選擇性地抹除資料。

條件式啟動

設定條件式啟動設定, 以設定存取保護原則的登入安全性需求。

根據預設, 系統會提供數個設定與預先設定的值和動作。您可以刪除其中一些專案, 例如 *Min OS 版本*。您也可以從 [選取一個] 下拉式清單中選取其他設定。

[[	[[[[
OS ■■	指定使用此應用程式的最大 iOS/iPadOS 作業系統。動作包括: ■ - 如果裝置上的 iOS/iPadOS 版本不符合需求, 使用者會看到通知。此通知可以關閉。 ■■ - 如果裝置上的 iOS/iPadOS 版本不符合此需求, 將會封鎖使用者存取。 ■■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 此專案可能會出現多次, 且每個實例都支援不同的動作。 此原則設定格式支援 major.minor、major.minor.build、major.minor.build.revision。 **注意:** 應用程式必須Intune SDK 14.4.0 版或更新版本。

[[	]]]]
■ OS ■	指定使用此應用程式的最低 iOS/iPadOS 作業系統。<i>動作</i> 包括： ● ■ - 如果裝置上的 iOS/iPadOS 版本不符合需求, 使用者會看到通知。此通知可以關閉。 ● ■■ - 如果裝置上的 iOS/iPadOS 版本不符合此需求, 將會封鎖使用者存取。 ● ■■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 此專案可能會出現多次, 且每個實例都支援不同的動作。 此原則設定格式支援 major.minor、major.minor.build、major.minor.build.revision。 **注意:** 應用程式必須Intune SDK 7.0.1 版或更新版本。
PIN ■■■■	指定使用者在採取設定的動作之前, 必須成功輸入 PIN 的嘗試次數。如果使用者在 PIN 嘗試次數上限之後無法成功輸入 PIN 碼, 使用者必須在成功登入其帳戶並完成多重要素驗證之後重設其 PIN, (需要 MFA) 挑戰。此原則設定格式支援正整數。<i>動作</i> 包括： ● ■ PIN - 使用者必須重設其 PIN。 ● ■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 預設值 = 5
■■■	受原則管理的應用程式可以離線執行的分鐘數。指定重新檢查應用程式存取需求之前) 分鐘 (的時間。<i>動作</i> 包括： ● ■■ (■) - 受原則管理的應用程式可以離線執行的分鐘數。指定重新檢查應用程式存取需求之前) 分鐘 (的時間。設定的期間到期之後, 應用程式會封鎖對公司或學校資料的存取, 直到有網路存取權。封鎖存取的離線寬限期計時器會在應用程式發行者金鑰鏈中的所有應用程式之間共用。此原則設定格式支援正整數。 預設值 = 720 分鐘 (12 小時) ●) (■■■ - 在系統管理員) 定義這幾天 (離線執行之後, 應用程式將要求使用者連線到網路並重新驗證。如果使用者成功驗證, 他們可以繼續存取其資料, 並重設離線間隔。如果使用者無法驗證, 應用程式將會執行使用者帳戶和資料的選擇性抹除。如需使用選擇性抹除移除哪些資料的詳細資訊, 請參閱如何只抹除Intune受控應用程式中的公司資料。針對抹除資料的離線寬限期計時器, 會根據上次簽入Intune服務, 個別計算每個應用程式的資料。此原則設定格式支援正整數。 預設值 = 90 ■ 此專案可能會出現多次, 且每個實例都支援不同的動作。
■/Root ■■■■	此設定沒有要設定的值。<i>動作</i> 包括： ● ■■ - 防止此應用程式在已越獄或 Root 破解的裝置上執行。使用者仍可繼續使用此應用程式進行個人工作, 但必須使用不同的裝置來存取此應用程式中的工作或學校資料。 ● ■■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。

[[	]]]]
■	此設定沒有要設定的值。動作 包括： ● ■ - 當我們確認使用者已在 Azure Active Directory 中停用時，應用程式會封鎖對公司或學校資料的存取。 ● ■ - 當我們確認使用者已在 Azure Active Directory 中停用時，應用程式將會執行使用者帳戶和資料的選擇性抹除。
■	指定最低應用程式版本值的值。動作 包括： ● ■ - 如果裝置上的應用程式版本不符合需求，使用者會看到通知。此通知可以關閉。 ● ■ - 如果裝置上的應用程式版本不符合需求，則會封鎖使用者存取。 ● ■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 由於應用程式之間通常會有不同的版本控制配置，因此請建立一個以一個應用程式為目標之最低應用程式版本的原則 (例如，<i>Outlook 版本原則</i>)。 此專案可能會出現多次，且每個實例都支援不同的動作。 此原則設定格式支援 major.minor、major.minor.build、major.minor.build.revision。 **注意:** 應用程式必須Intune SDK 7.0.1 版或更新版本。 此外，您可以設定終端使用者可在 ■ 取得企業營運 (LOB) 應用程式的更新版本。終端使用者會在 [■ 條件式啟動] 對話方塊中看到此資訊，這會提示終端使用者更新為最低版本的 LOB 應用程式。在 iOS/iPadOS 上，這項功能需要將應用程式整合 (或使用包裝工具組裝，) 搭配適用於 iOS 的 Intune SDK v. 10.0.7 或更新版本。若要設定終端使用者應該更新 LOB 應用程式的位置，應用程式需要使用金鑰 傳送給它的受控應用程式設定原則。<code>com.microsoft.intune.myappstore</code> 傳送的值會定義終端使用者將從哪個存放區下載應用程式。如果應用程式是透過 公司入口網站部署，則值必須是 <code>CompanyPortal</code>。針對任何其他存放區，您必須輸入完整的 URL。
■ SDK ■	指定 Intune SDK 版本的最小值。動作 包括： ● ■- 如果應用程式的Intune應用程式保護原則 SDK 版本不符合需求，則會封鎖使用者存取。 ● ■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 若要深入瞭解Intune應用程式保護原則 SDK，請參閱 Intune App SDK 概觀。由於應用程式之間通常Intune SDK 版本不同，因此請建立一個以一個應用程式為目標Intune SDK 版本 Intune原則 (例如，<i>Intune Outlook</i>) 的 SDK 版本原則。 此專案可能會出現多次，且每個實例都支援不同的動作。

[[	[[[[
■ ()	指定模型識別碼的分號分隔清單 ()。這些值不區分大小寫。 動作包括： ● ■ (■) - 只有符合指定裝置型號的裝置才能使用應用程式。所有其他裝置型號都會遭到封鎖。 ● ■ (■) - 與應用程式相關聯的使用者帳戶會從裝置抹除。 如需使用此設定的詳細資訊，請參 閱條件式啟動動作。
■	應用程式防護原則可以利用 Intune-MTD 連接器。指定可接受使用此應用程式的最大威脅層級。威脅取決於您在終端使用者裝置上選擇的 Mobile Threat Defense (MTD) 廠商應用程式。指定 [安全]、[低]、[中] 或 [高]。受保護不需要裝置上的威脅，而且是最嚴格的可設定值，而 High 基本上需要使用中 Intune 對 MTD 連線。動作包括： ● ■ - 如果您在終端使用者裝置上選擇的 Mobile Threat Defense (MTD) 廠商應用程式所決定的威脅層級不符合此需求，則會封鎖使用者存取。 ● ■ - 與應用程式相關聯的使用者帳戶會從裝置抹除。 **注意:** 應用程式必須Intune SDK 12.0.15 版或更新版本。 如需使用此設定的詳細資訊，請參閱 為未註冊的裝置啟用 MTD。

深入了解

- 瞭解 [LinkedIn Microsoft 應用程式中的資訊和功能](#)。
- 在 [Microsoft 365 藍圖頁面](#) 上瞭解LinkedIn帳戶連線版本。
- 瞭解如何 [設定LinkedIn帳戶連線](#)。
- 如需使用者LinkedIn與 Microsoft 公司或學校帳戶之間共用之資料的詳細資訊，請 [參閱在公司或學校的 Microsoft 應用程式中LinkedIn](#)。

使用 Intune 中的應用程式保護原則條件式啟動動作選擇性清除資料

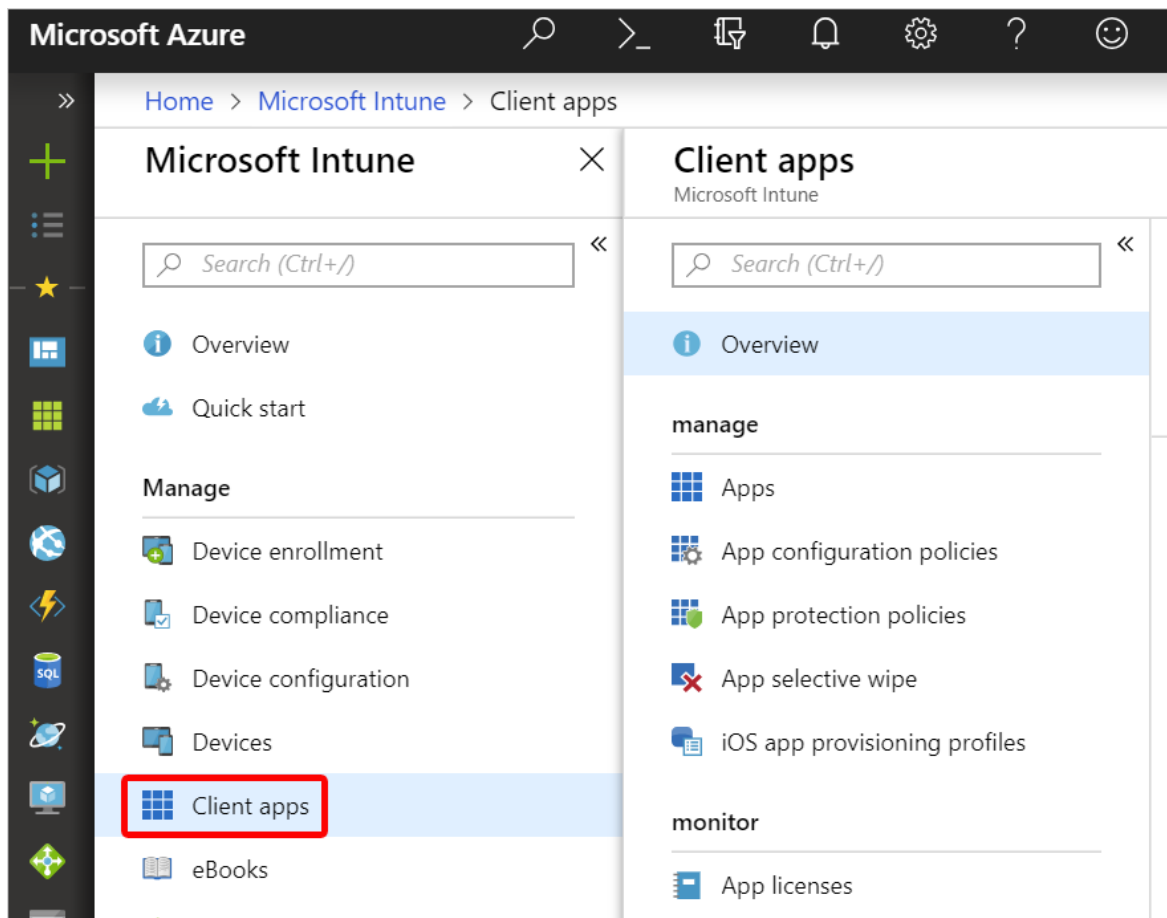
2022/9/27 •

Intune 應用程式保護原則中的條件式啟動動作可讓組織在特定裝置或應用程式條件不符合時，封鎖存取權或擦除組織資料。

您可以明確選擇從使用者的裝置中清除公司的公司資料，作為使用這些設定進行非法規遵從性時採取的動作。針對某些設定，您可以設定多個動作，例如封鎖存取，以及根據不同的指定值來清除資料。

使用條件式啟動動作建立應用程式保護原則

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [app > 應用程式防護原則]。
3. 按一下 [建立原則]，然後選取原則的裝置平臺。
4. 按一下 [設定必要設定]，以查看可針對原則設定的設定清單。
5. 在 [設定] 窗格中向下，您將會看到一個以可編輯的資料表為 **條件式啟動** 的區段。



6. 選取 ****[設定]，然後輸入使用者必須符合的 ****[值]，才能登入您的公司應用程式。
7. 若使用者不符合您的需求，請選取您要採取的 **動作**。在某些情況下，單一設定可以設定多個動作。如需詳細資訊，請參閱 [如何建立和指派應用程式保護原則](#)。

原則設定

應用程式保護原則設定表格具有 **設定**、**值** 及 **動作** 的欄。

iOS 原則設定

若為 iOS/iPadOS，您可以使用 [**設定**] 下拉式清單，設定下列設定的動作：

- 最大 PIN 嘗試次數
- 離線寬限期
- 已越獄/有根裝置
- 作業系統最大版本
- 作業系統最小版本
- 最小應用程式版本
- 最小 SDK 版本
- 裝置模型 (s)
- 允許的最大裝置威脅層級
- 停用帳戶

若要使用 **裝置模型 (s)** 設定，請輸入分號分隔的 iOS/iPadOS 模型識別碼清單。這些值不區分大小寫。除了 Intune '裝置模型 (s)' 輸入的報告之外，您還可以在此[協力廠商 GitHub 存放庫](#)中找到 iOS/iPadOS 模型識別碼。範例輸入：*iPhone5, 2*、*iPhone5, 3*

在使用者裝置上，Intune 用戶端會根據在 Intune 中為應用程式保護原則所指定之裝置模型字串的簡單相符，採取行動。相符完全取決於裝置報告。您 (IT 系統管理員) 鼓勵您根據各種裝置製造商和模型來測試此設定，並以小型使用者群組為目標，以確保預定行為發生。預設值為 [**未設定**]。

設定下列其中一個動作：

- 允許指定的 (區塊非指定)
- 允許指定的 (擦除非指定的)

如果 IT 系統管理員輸入不同的 iOS/iPadOS 模型 (識別碼清單) 為相同 Intune 使用者的相同應用程式的原則，會發生什麼事？

在設定的值的兩個應用程式保護原則之間發生衝突時，Intune 通常會採用最具限制性的方法。因此，由目標 Intune 使用者開啟的目標應用程式所傳送的結果原則，會是 *原則 A* 與原則 B 中所列的 iOS/iPadOS 模型識別碼 (s) 的交集，且 *原則 B* 會以相同的應用程式/使用者組合為目標。例如，*policy a* 指定 "iPhone5, 2; iPhone5, 3"，當 *原則 B* 指定 "iPhone5, 3" 時，所產生的原則 *是原則 A* 和 *policy B* 所設定的 Intune 使用者會是 "iPhone5, 3"。

Android 原則設定

針對 Android，您可以使用 **設定** 下拉式功能表設定下列設定的動作：

- 最大 PIN 嘗試次數
- 離線寬限期
- 已越獄/有根裝置
- 作業系統最小版本
- 作業系統最大版本
- 最小應用程式版本
- 最小修補程式版本
- 裝置製造商 (s)
- SafetyNet 裝置證明
- 需要在應用程式上進行威脅掃描
- 最低公司入口網站版本
- 允許的最大裝置威脅層級

- 停用帳戶
- 需要裝置鎖定

使用 **Min 公司入口網站版本**，您可以指定在使用者裝置上強制執行的特定最小定義版本公司入口網站。此條件式啟動設定可讓您設定值以 **封鎖存取**、**清除資料**，以及在未符合每個值時 **警告** 盡可能採取的動作。此值的可能格式遵循 *[主要] 的模式*。[小調]，[主要]。[小調]。[組建] 或 [主要]。[小調]。[組建]。[Revision]。假設某些使用者可能不想強制更新點上的應用程式，當您設定此設定時，「警告」選項可能是理想的選項。Google Play 存放區只會傳送應用程式更新的增量位元組，但這仍是大量的資料，如果使用者在更新時，可能不想要使用這些資料。強制更新，進而下載更新的應用程式可能會在更新時導致意外的資料費用。**[最小公司入口網站版本]** 設定 (若已設定) 會影響任何取得公司入口網站版本 5.0.4560.0，以及任何未來版本公司入口網站的使用者。此設定對使用版本低於此功能發行之版本的公司入口網站使用者將不會有任何影響。使用者在其裝置上使用自動更新的使用者可能無法看到來自此功能的任何對話方塊，因為它們可能會在最新的公司入口網站版本上。只有已註冊和 unenrolled 裝置的應用程式保護，此設定才為 Android。

若要使用 **Device manufacturer (s)** 設定，請輸入以分號分隔的 Android 廠商清單。這些值不區分大小寫。除了 Intune 報告之外，您還可以在 [裝置設定] 底下找到裝置的 Android 生產廠商。

範例輸入：製造商 A;製造商 B

NOTE

以下是一些常見製造商從使用 Intune 的裝置報告，可用作輸入：Asus;BlackberryBq;Gionee;雲端Hmd global;HtcHuawei;Infinix;Kyocera;Lemobile;LenovoLge;Motorola;Oneplus;Oppo;三星井電池組Tecno;Vivo;Vodafone;Xiaomi;Zte;Zuk

在使用者裝置上，Intune 用戶端會根據在 Intune 中為應用程式保護原則所指定之裝置模型字串的簡單相符，採取行動。相符完全取決於裝置報告。您 (IT 系統管理員) 鼓勵您根據各種裝置製造商和模型來測試此設定，並以小型使用者群組為目標，以確保預定行為發生。預設值為 [未設定]。

設定下列其中一個動作：

- 允許在非指定的) 上指定 (區塊)
- 允許在非指定的) 上指定 (清除)

如果 IT 系統管理員輸入不同於相同 Intune 使用者之相同應用程式的原則 (s) 不同清單，會發生什麼情況？

在設定的值的兩個應用程式保護原則之間發生衝突時，Intune 通常會採用最具限制性的方法。因此，將結果原則傳送至目標 Intune 使用者開啟的目標應用程式，將會是 *原則 A* 中所列的 Android 廠商和原則 B 中所列的與 *原則 B* 的交集，其目標是相同的應用程式/使用者組合。例如，*原則 A* 指定 "Google;Samsung"，當 *原則 B* 指定 "google" 時，由雙方 *原則 A* 和 *policy B* 的 Intune 使用者所設定的結果原則都會是 "google"。

其他設定和動作

根據預設，表格會將列填入設定為 **離線寬限期** 和 **最大 PIN 嘗試** 的列 (如果 [需要存取 Pin] 設定為 [是])。

若要設定設定，請從 [設定] 欄底下的下拉式清單中選取設定。選取設定之後，如果必須設定值，就會在同一列的 [值] 欄中啟用可編輯的文字方塊。此外，下拉式清單會在 [動作] 欄 (適用於設定的條件式啟動動作集合) 下啟用。

下列清單提供一般動作清單：

- **封鎖存取** – 封鎖使用者存取企業應用程式。
- **擦除資料** – 從使用者的裝置中清除公司資料。
- **警告** – 將使用者對話方塊提供給使用者，做為警告訊息。

在某些情況下 (例如 [最小作業系統版本] 設定)，您可以設定設定，以根據不同的版本號碼執行所有適用的動作。

SETTING	VALUE	ACTION	
Max PIN attempts	5	Reset PIN	•
Offline grace period	720	Block access (minutes)	•
Offline grace period	90	Wipe data (days)	•
Jailbroken/rooted devices		Block access	•
Min OS version	6.0	Wipe data	•
Min OS version		Select one	•
Select one		Block access	
		Wipe data	
		Warn	

設定完全設定後，列將會出現在唯讀的視圖中，且可隨時進行編輯。此外，列會顯示 [設定] 欄中的選取範圍。已設定的設定，而且不允許多重動作可用於 dropdown 中的選取範圍。

後續步驟

深入瞭解 Intune 應用程式保護原則的詳細資訊，請參閱：

- [如何建立及部署應用程式保護原則](#)
- [iOS/iPadOS 應用程式保護原則設定](#)
- [Microsoft Intune 中的 Android 應用程式保護原則設定](#)

如何在 Intune 應用程式保護原則中建立例外狀況 (應用程式) 資料轉移原則

2022/9/27 •

以管理員身分，您可以在 Intune 應用程式保護原則 (應用程式) 資料傳輸原則中建立例外狀況。例外狀況可讓您明確選擇哪些未受管理的應用程式可以在受管理的應用程式中傳輸資料。您的 IT 必須信任您在例外狀況清單中包含的非管理應用程式。

WARNING

您負責變更資料傳送例外狀況原則。此原則的新增功能可讓未受 Intune 管理的未受管理的應用程式 (應用程式存取受管理的應用程式保護的資料。存取受保護的資料可能會導致資料安全性洩漏。針對您的組織必須使用的應用程式，新增資料傳輸例外狀況，但不支援 Intune APP (應用程式保護原則)。此外，只為您未考慮成為資料洩漏風險的應用程式新增例外狀況。

在 Intune 應用程式保護原則中，設定 [允許應用程式將資料傳送至其他應用程式至原則受管理的應用程式] 表示應用程式只能將資料傳送給 Intune 所管理的應用程式。如果您需要允許將資料傳輸到不支援 Intune 應用程式的特定應用程式，您可以使用 [選取要免除的應用程式] 來建立此原則的例外狀況。免除允許 Intune 所管理的應用程式會根據 URL 通訊協定 (iOS/iPadOS) 或套件名稱 (Android)，來呼叫未受管理的應用程式。根據預設，Intune 會將重要的原生應用程式新增至此例外狀況清單。

NOTE

修改或新增資料傳送原則例外不會影響其他應用程式保護原則，例如剪下、複製及貼上限制。

iOS 資料傳輸例外狀況

針對 iOS/iPadOS 的原則，您可以依據 URL 通訊協定設定資料傳送例外狀況。若要新增例外狀況，請查看應用程式開發人員所提供的檔，以尋找有關支援之 URL 通訊協定的資訊。如需 iOS/iPadOS 資料傳輸例外狀況的相關資訊，請參閱 [iOS/iPadOS 應用程式保護原則設定-資料傳輸例外](#)。

NOTE

Microsoft 不具備手動尋找建立協力廠商應用程式之應用程式例外之 URL 通訊協定的方法。

Android 資料傳輸例外狀況

針對針對 Android 的原則，您可以依應用程式套件名稱來設定資料傳輸例外狀況。您可以在 [您想要新增例外狀況的應用程式] 中，檢查 Google Play store 頁面以尋找應用程式套件名稱。如需 Android 資料傳輸例外狀況的相關資訊，請參閱 [Android 應用程式保護原則設定-資料傳輸例外](#)。

TIP

您可以流覽至 Google Play 商店上的應用程式，來尋找應用程式的封裝識別碼。套件識別碼包含在應用程式頁面的 URL 中。例如，Microsoft Word 應用程式的套件識別碼為 .com。

範例

將 webex 套件新增為 MAM 資料傳送原則的例外狀況，受管理的 Outlook 電子郵件中的 webex 連結可直接在

Webex 應用程式中開啟。在其他非管理的應用程式中，資料傳輸仍受到限制。

- iOS/iPadOS **webex** 範例：若要免除 **Webex** 應用程式，使其允許 Intune 受管理的應用程式呼叫，您必須為下列字串新增資料傳輸例外狀況：`wbx`
- iOS/iPadOS **地圖** 範例：若要免除原生 **地圖** 應用程式，以便 Intune 受管理的應用程式可呼叫它，您必須為下列字串新增資料傳輸例外狀況：`maps`
- Android **webex** 範例：若要免除 **Webex** 應用程式，以便 Intune 受管理的應用程式可呼叫它，您必須為下列字串新增資料傳輸例外狀況：`com.cisco.webex.meetings`
- Android **sms** 範例：若要免除原生 SMS 應用程式，以便在不同的郵件應用程式和 Android 裝置間 Intune 受管理的應用程式，您必須為下列字串新增資料傳輸例外狀況：`com.google.android.apps.messaging`

`com.android.mms`

`com.samsung.android.messaging`

後續步驟

- [建立及部署應用程式保護原則](#)
- [iOS/iPadOS 應用程式保護原則設定-資料傳輸例外](#)
- [Android 應用程式保護原則設定-資料傳輸例外](#)

如何在 Microsoft Intune 中驗證應用程式保護原則安裝程式

2022/9/27 •

驗證應用程式保護原則已正確設定且正常運作。此指南適用於入口網站中的應用程式保護原則。

檢查是否有徵兆

使用者不太可能報告問題，因為應用程式保護是資料保護工具。如果應用程式保護設定有問題，使用者就會有不受限制的存取權，因為它們不會有應用程式保護，也不會知道有問題。基於這個理由，我們建議您使用可故意測試應用程式保護限制之一小組使用者的應用程式保護原則，來驗證應用程式保護設定。

檢查項目

如果測試顯示您的應用程式保護原則行為未如預期運作，請檢查下列專案：

- 使用者是否已取得應用程式保護的授權？
- 使用者是否有 Microsoft 365 的授權？
- 是所期望的使用者應用程式保護應用程式的狀態。已 存回應用程式的可能狀態，且 未 存回。

使用者應用程式保護狀態

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式 >] [監視 >] 應用程式防護狀態]，然後選取 [指派的使用者] 磚。
3. 在 [應用程式報告] 頁面上，選取 [選取使用者] 以顯示使用者和群組的清單。
4. 在清單中搜尋並選取使用者，然後選擇 [選取使用者]。在 [應用程式報告] 窗格的頂端，您可以看到使用者是否已取得應用程式保護的授權。您也可以查看使用者是否有 Microsoft 365 的授權，以及所有使用者裝置的應用程式狀態。

處理方式

以下是根據使用者狀態採取的動作：

- 如果使用者未取得應用程式保護的授權，請將 [Intune 授權](#) 指派給使用者。
- 如果使用者未獲授權 Microsoft 365，請取得使用者的 [授權](#)。
- 如果使用者的應用程式列為 未 存回的，請檢查您是否已正確設定該應用程式的 [應用程式保護原則](#)。
- 確定這些條件會在您要套用 [應用程式保護原則](#) 的所有使用者上套用。

請參閱

- [何謂 Intune app protection 原則？](#)
- [包含 Intune 的授權](#)
- [將授權指派給使用者，讓他們可以在 Intune 中註冊裝置](#)
- [如何驗證您的應用程式保護原則設定](#)
- [如何監視應用程式保護原則](#)

了解應用程式保護原則傳遞時間表

2022/9/27 •

瞭解適用於應用程式保護原則的不同部署視窗，以瞭解何時應該在使用者裝置上顯示變更。

傳遞時程表摘要

應用程式防護原則 (應用程式) 傳遞取決於使用者的授權狀態及 Intune 服務註冊。

狀態	說明	時間 (小時)	說明？
租使用者未架	等候下一個重試間隔。使用者的應用程式保護不是作用。	24小時	當您未設定 Intune 租使用者時，就會發生此事件。
使用者未獲授權	等候下一個重試間隔。使用者的應用程式保護不是作用。	12小時-不過，在 Android 裝置上此間隔需要 Intune 應用程式 SDK 版本5.6.0 或更新版本。否則，如果是 Android 裝置，則間隔為24小時。	當您未授權使用者 Intune 時，就會發生此事件。
使用者未獲指派應用程式保護原則	等候下一個重試間隔。使用者的應用程式保護不是作用。	12 小時	當您未將應用程式設定指派給使用者時，就會發生此事件。
使用者指派的應用程式保護原則，但應用程式不會在應用程式保護原則中定義	等候下一個重試間隔。使用者的應用程式保護不是作用。	12 小時	當您未將應用程式新增至應用程式時，就會發生此事件。
已成功登錄 Intune MAM 的使用者	每個原則設定會套用應用程式保護。根據重試間隔進行更新	Intune 根據使用者負載定義的服務。通常為30分鐘。	會在使用者成功註冊應用程式設定的 Intune 服務時發生。

NOTE

重試間隔可能需要使用中的應用程式，這表示應用程式已啟動並在使用中。如果重試間隔為24小時，且使用者在48小時內啟動應用程式，則 Intune 應用程式 SDK 會在48時重試。

處理網路連通性問題

當使用者註冊因網路連線問題而失敗時，會使用加速重試間隔。Intune 應用程式 SDK 會在較長的時間間隔重試，直到此間隔變為60分鐘或連線成功為止。Intune 應用程式 SDK 將繼續以60分鐘的間隔重新嘗試，直到順利進行連線為止。然後，Intune 應用程式 SDK 會根據使用者狀態，傳回標準重試間隔。

後續步驟

將授權指派給使用者，讓他們可以在 Intune 中註冊裝置

保護應用程式擴充

2022/9/27 •

本文說明 Microsoft Intune 中擴充的應用程式保護原則。

Outlook 應用程式的增益集

Outlook 增益集可讓您將流行的應用程式與電子郵件用戶端整合。Outlook 的增益集可用於 Android 和 iOS/iPadOS 的 web、Windows、Mac 及 Outlook。Intune 應用程式 SDK 和 Intune 應用程式保護原則不包含管理 Outlook 增益集的支援，但是還有其他方法可以限制其使用。因為增益集是透過 Microsoft Exchange 管理的，所以使用者將能夠在 Outlook 和未受管理的增益集應用程式之間共用資料和郵件，除非其 Exchange 為使用者關閉增益集。

如果您想要讓使用者停止存取和安裝 Outlook 增益集 (這會影響所有 Outlook 用戶端)，請確定您在 Exchange 系統管理中心中對角色進行下列變更：

- 若要防止使用者安裝 Office 儲存增益集，請從這些增益集中移除「我的 Marketplace」角色。
- 若要防止使用者從側面載入增益集，請從這些增益集移除我的自訂應用程式角色。
- 若要防止使用者安裝所有增益集，請從這些增益集中移除我的自訂應用程式和我的 Marketplace 角色。

這些指示適用於 Microsoft 365、Exchange 2016、Exchange 2013 的 Outlook 網頁版、Windows、Mac 及行動裝置。

- 深入瞭解[Outlook 的增益集](#)。
- 深入瞭解[如何指定管理員和使用者，以便在 Outlook 應用程式中安裝及管理增益集](#)。

Microsoft 應用程式的 LinkedIn 帳戶連線

LinkedIn 帳戶連線允許使用者在某些 Microsoft 應用程式中查看公用 LinkedIn 設定檔資訊。根據預設，您的使用者可以選擇連接其 LinkedIn 和 Microsoft 工作或學校帳戶，以查看其他 LinkedIn 設定檔資訊。

NOTE

LinkedIn 整合目前不適用於美國政府客戶和組織，其具有在澳大利亞、加拿大、中國、法國、德國、德國、韓國、南美、日本和南非的 Exchange Online 信箱。

Intune SDK 和 Intune 應用程式保護原則不包含管理 LinkedIn 帳戶連線的支援，但是還有其他管理方式。您可以為整個組織停用 LinkedIn 帳戶連線，也可以為組織中所選的使用者群組啟用 LinkedIn 帳戶連線。這些設定會影響所有平臺上 Microsoft 365 應用程式的 LinkedIn 連線，(網頁、行動裝置和桌面)。您可以：

- 啟用或停用入口網站中您租使用者的 LinkedIn 帳戶連線。
- 使用群組原則來啟用或停用組織之 Office 2016 應用程式的 LinkedIn 帳戶連線。

如果為您的租使用者啟用 LinkedIn 整合，當您組織中的使用者連接其 LinkedIn 和 Microsoft 單位或學校帳戶時，會有兩個選項：

- 他們可以授與兩個帳戶間共用資料的許可權。這表示他們會授與其 LinkedIn 帳戶的許可權，以與其 Microsoft 公司或學校帳戶共用資料，以及他們的 Microsoft 工作或學校帳戶，以與其 LinkedIn 帳戶共用資料。與 LinkedIn 共用的資料會保留線上服務。
- 他們可以將只從其 LinkedIn 帳戶共用資料的許可權授予其 Microsoft 工作和學校帳戶。

如果使用者 consents 在帳戶間共用資料，就像 Office 增益集一樣，LinkedIn 整合會使用現有的 Microsoft Graph APIs。LinkedIn 整合只會使用可 Office 增益集的 APIs 子集，並支援各種排除。

MICROSOFT GRAPH Ⅱ (Ⅱ)	Ⅱ
人員 的讀取權限	允許此應用程式讀取與登入使用者相關之人員的計分清單。清單可以包含 [本地連絡人]、「社交網路」的連絡人或您組織的目錄，以及最近通訊 (的人員，例如電子郵件和 Skype)。
行事曆的讀取權限	允許應用程式讀取使用者行事曆中的事件。包括已登入使用者行事曆中的會議、他們的時間、地點及出席者。
使用者設定檔 的讀取權限	允許使用者登入 app，並允許此應用程式讀取登入使用者的設定檔。它也可讓應用程式讀取已登入使用者的基本公司資訊。
訂閱	此範圍無法使用，尚未使用。它包含使用者組織提供給 Microsoft 應用程式和服務的訂閱，例如 Microsoft 365。
深入解析	此範圍無法使用，尚未使用。根據使用 Microsoft 服務，包含已登入使用者的帳戶相關的興趣。

深入了解

- 深入瞭解 [Microsoft 應用程式中的 LinkedIn 資訊和功能](#)。
- 深入瞭解[Microsoft 365 藍圖頁面](#)上的 LinkedIn 帳戶連線版本。
- 瞭解如何設定 [LinkedIn 帳戶](#)連線。
- 如需使用者 LinkedIn 和 Microsoft 工作或學校帳戶之間共用之資料的詳細資訊，請參閱在 [您的公司或學校的 microsoft 應用程式中 LinkedIn](#)。

如何監視應用程式保護原則

2022/9/27 •

您可以從 Intune 中的 [應用程式保護] 窗格，監視已 Intune 套用至使用者的應用程式保護原則狀態。此外，您可以找到受應用程式保護原則影響的使用者、原則合規性狀態，以及使用者可能遇到之任何問題的相關資訊。

監視應用程式保護原則有三個不同的位置：

- 摘要檢視
- 詳細檢視
- 報告檢視

應用程式防護資料會保留至少 90 天。過去 90 天記憶體回 Intune 服務的任何應用程式實例都會包含在應用程式保護狀態報表中。*應用程式實例* 是唯一的使用者 + 應用程式 + 裝置。

NOTE

如需詳細資訊，請 [參閱如何建立和指派應用程式保護原則](#)。

摘要檢視

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [應用程式] > [監視] > [應用程式防護狀態]。

下列清單提供應用程式保護狀態的詳細資料：

- **指派的使用者：**貴公司中使用與工作內容中原則相關聯且受到保護和授權之應用程式的指派使用者總數，以及未受保護和未授權的指派使用者。
- **已標幟的使用者：**裝置發生問題的使用者數目。已越獄 (iOS/iPadOS) 和 root root (Android) 裝置會在 **標幟的使用者** 下回報。此外，如果 IT 系統管理員) 開啟，具有 Google SafetyNet 裝置證明所標幟之裝置的使用者 (，則會在此處回報。
- **具有潛在有害應用程式的使用者：**Google Play Protect 在其 Android 裝置上偵測到有害應用程式的使用者數目。
- **iOS 的使用者狀態 和 Android 的使用者狀態：**在相關平臺的工作內容中使用已指派原則的應用程式的使用者數目。此資訊會顯示原則所管理的使用者數目，以及使用工作內容中任何原則未設為目標之應用程式的使用者數目。您可以考慮將這些使用者新增至原則。
- **Top Protected iOS/iPadOS Apps and Top Protected Android Apps：**根據最常使用的 iOS/iPadOS 和 Android 應用程式，此資訊會依平臺顯示受保護和未受保護的應用程式數目。
- **最常設定的 iOS/iPadOS 應用程式但不 註冊，以及 最常設定的 Android 應用程式無註冊：**根據最常使用的 iOS/iPadOS 和未註冊裝置的 Android 應用程式，此資訊會顯示依平臺 (設定的應用程式數目，如同使用應用程式設定原則) 一樣。

NOTE

如果您每個平臺有多個原則，當使用者至少有一個原則指派給他們時，就會被視為由原則管理。

詳細檢視

您可以選擇 [已標幟的使用者] 圖格和 [具有潛在有害應用程式的使用者] 圖格，以取得摘要的詳細檢視。

標幟的使用者

詳細檢視會顯示錯誤訊息、錯誤發生時所存取的應用程式、受影響的裝置 OS 平臺，以及時間戳記。此錯誤通常是針對 (iOS/iPadOS) 或 root root 破解 (Android) 裝置。此外，此處也會報告具有已標示為「SafetyNet 裝置證明」條件式啟動檢查之裝置的使用者，以及 Google 所報告的原因。若要從報表中移除使用者，裝置本身的狀態必須已變更，這會在下一次根偵測檢查 (或越獄檢查/SafetyNet 檢查之後發生，) 需要回報正面結果。如果裝置已真正修復，當窗格重載時，就會重新整理 [已標幟的使用者] 報表。

具有潛在有害應用程式的使用者

此處會報告具有裝置且已標示為 [應用程式上需要威脅掃描] 條件式啟動檢查的使用者，其中包含 Google 所報告的威脅類別。如果此報告中列出的應用程式是透過Intune部署，請連絡應用程式的應用程式開發人員，或移除應用程式不被指派給您的使用者。詳細檢視會顯示：

- **使用者：**使用者的名稱。
- **應用程式套件標識符：**這是Android OS 唯一決定應用程式的方式。
- **如果應用程式已啟用 MAM：**是否透過Microsoft Intune部署應用程式。
- **威脅類別：**此應用程式屬於 Google 判定的威脅類別。
- **電子郵件：**使用者的電子郵件。
- **裝置名稱：**與使用者帳戶相關聯之任何裝置的名稱。
- **時間戳記：**這是 Google 與可能有害應用程式Microsoft Intune上次同步處理的日期。

報告檢視

您可以在 [應用程式防護 狀態] 窗格的頂端找到相同的報告。若要檢視這些報告，請選取 [應用程式 > 監視器 > 應用程式防護狀態 > [報告]]。[報表] 窗格會根據使用者和應用程式提供數個報表，包括下列各項：

使用者報告

您可以搜尋單一使用者，並檢查該使用者的合規性狀態。[應用程式報告] 窗格會顯示所選使用者的下列資訊：

- **圖示：**顯示應用程式狀態是否為最新狀態。
- **應用程式名稱：**應用程式的名稱。
- **裝置名稱：**與使用者帳戶相關聯的裝置。
- **裝置類型：**裝置正在執行的裝置或作業系統類型。
- **原則：**與應用程式相關聯的原則。
- **狀態：**
 - **簽入：**原則已部署至使用者，且應用程式至少用於工作內容一次。
 - **未簽入：**原則已部署至使用者，但該應用程式自此之後未在工作內容中使用。
- **上次同步處理：**上次與Intune同步處理應用程式的時間。

NOTE

[■] 資料行在主控制台內的 [使用者狀態] 報表和 [應用程式保護原則可匯出] .csv報表中都代表相同的值。差異在於兩個報表中值之間的同步處理延遲很小。

上次同步處理中參考的時間是Intune上次看到應用程式實例的時間。當使用者啟動應用程式時，可能會在該啟動時間通知Intune應用程式保護服務，視上次簽入的時間而定。請參閱[應用程式保護原則簽入的重試間隔時間](#)。如果使用者在最後一次簽入間隔中未使用該特定應用程式，(使用) 通常為 30 分鐘，而且他們啟動應用程式，則：

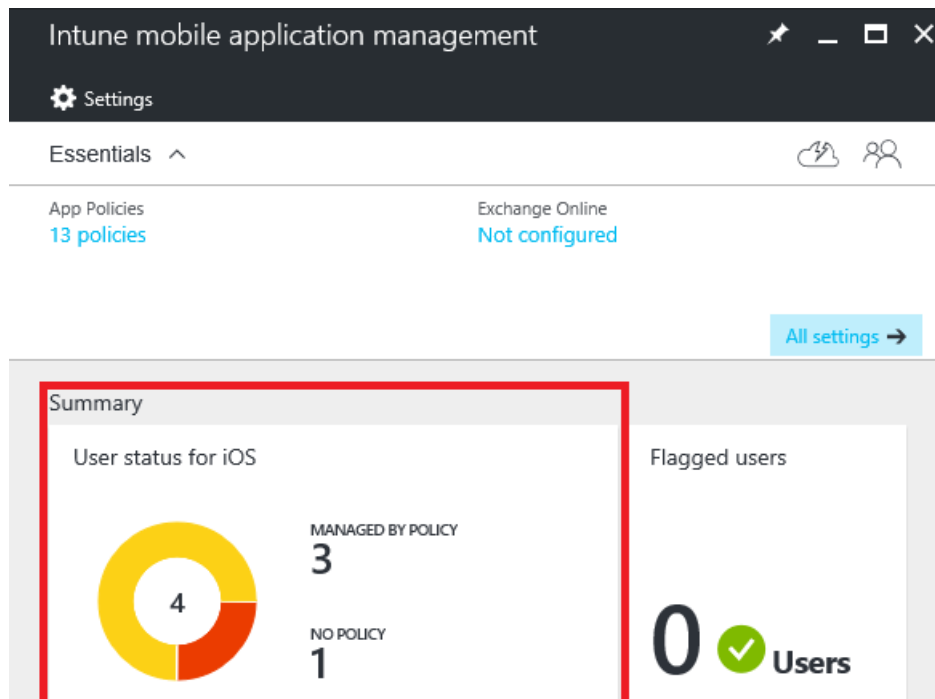
- 應用程式保護原則可匯出.csv報表有最新的時間，(最少) 1 分鐘到 30 分鐘，(最大)。
- 使用者狀態報表會立即有最新的時間。

例如，假設有目標且授權的使用者在下午 12:00 啟動受保護的應用程式：

- 如果這是第一次登入，這表示使用者之前已登出，而且沒有向Intune註冊應用程式實例。使用者登入之後，使用者會取得新的應用程式實例註冊，而且可以立即簽入 (與先前針對未來簽入) 所列的相同時間延遲。因此，上次同步處理時間是使用者狀態報表中的下午 12:00，下午 12:01 (或 12:30 在應用程式保護原則報告中)。
- 如果使用者只是啟動應用程式，則回報的上次同步時間取決於使用者上次簽入的時間。

若要查看使用者的報告，請遵循下列步驟：

1. 若要選取使用者，請選擇 [使用者狀態 摘要] 圖格。



2. 在 [應用程式報告] 窗格中，選擇 [選取要 搜尋Azure Active Directory使用者的使用者]。

App reporting

Select user

APP NAME ^

DEVICE NAME ^

DEVICE TYPE ^

No user selected

3. 從清單中選取使用者。您可以查看該使用者合規性狀態的詳細資料。

NOTE

如果您搜尋的使用者沒有部署 MAM 原則，您會看到一則訊息，通知您使用者並非任何 MAM 原則的目標。

應用程式報告

您可以依平臺和應用程式進行搜尋，然後此報告會提供兩個不同的應用程式保護狀態，您可以在產生報表之前選取這些狀態。狀態可以是 [受保護] 或 [未受保護]。

- 受控 MAM 活動的使用者狀態 (受保護的)：此報告會依每位使用者概述每個受控 MAM 應用程式的活動。它會針對每位使用者顯示 MAM 原則的目標所有應用程式，以及每個應用程式在 MAM 原則中簽入時的狀態。此報告也包含以 MAM 原則為目標，但從未簽入的每個應用程式狀態。
- Unmanaged MAM 活動的使用者狀態 (未受保護的)：此報告會依每位使用者列出目前未受管理之已啟用 MAM 的應用程式活動。這可能是因為：
 - 這些應用程式正由使用者使用，或是目前不是 MAM 原則目標的應用程式使用。
 - 所有應用程式都會簽入，但不會取得任何 MAM 原則。

The screenshot displays two side-by-side windows from the Microsoft Intune console. The left window, titled 'App protection app report', shows filters for Platform (iOS), App (Outlook), and Status (Unprotected). Below these are fields for USER and EMAIL. The right window, titled 'App reporting', shows a message 'User is licensed for Microsoft Intune.' and a table with columns: APP NAME, DEVICE NAME, DEVICE TYPE, POLICIES, and STATUS. The table lists three apps: Excel, PowerPoint, and Word, all on Android devices with no policies applied and a status of 'Not checked in'.

APP NAME	DEVICE NAME	DEVICE TYPE	POLICIES	STATUS
Excel		Android	None	Not checked in
PowerPoint		Android	None	Not checked in
Word		Android	None	Not checked in

使用者設定報告

根據選取的使用者，此報告會提供使用者已收到之任何應用程式設定的詳細資料。

應用程式組態報告

根據選取的平臺和應用程式，此報告提供哪些使用者已收到所選應用程式設定的詳細資料。

適用於 Windows 資訊保護的應用程式學習報表

此報表顯示哪些應用程式嘗試跨越原則界限。

適用於 Windows 資訊保護的網站學習

此報表顯示哪些網站嘗試跨越原則界限。

匯出應用程式保護活動

您可以將所有應用程式保護原則活動匯出至單一.csv檔案。這有助於分析從使用者回報的所有應用程式保護狀態。應用程式保護.csv檔案會顯示：

- 使用者：使用者的名稱。
- 電子郵件：使用者的電子郵件。
- 應用程式：應用程式的名稱。
- 應用程式版本：應用程式的版本。
- 裝置名稱：與使用者帳戶相關聯之任何裝置的名稱。
- 裝置製造商：這會列出裝置的製造商 (Android僅)。
- 裝置型號：這會列出僅) 裝置 (Android製造商)。
- Android修補程式版本：上次Android安全性修補的日期。
- AAD 裝置識別碼：如果裝置已加入 AAD，就會填入此資料行。
- MDM 裝置識別碼：如果裝置已Microsoft Intune MDM 註冊，就會填入此資料行。
- 平臺：作業系統。

- 平臺版本：作業系統版本。
- 管理類型：裝置上的管理類型。例如，Android Enterprise、Unmanaged 或 MDM。
- 應用程式保護狀態：未受保護或受保護。
- 原則：與應用程式相關聯的應用程式保護原則。
- 上次同步處理：上次與Microsoft Intune同步處理應用程式的時間。
- 合規性狀態：使用者裝置上的應用程式是否符合任何以應用程式為基礎的條件式存取原則。

請遵循下列步驟來產生應用程式保護.csv檔案或應用程式組態 .csv檔案：

1. 在 [Intune行動應用程式管理] 窗格中，選擇 [應用程式防護報告]。

Intune mobile application management

Settings App protection...

Essentials ^

App Policies 13 policies Exchange Online Not configured

All settings →

Summary

User status for iOS

MANAGED BY POLICY 3

NO POLICY 1

Flagged users

0 ✓ Users

2. 選擇 [是] 以儲存報表，然後選擇 [另存新檔]。選取您要儲存報表的資料夾。

Save Report

Would you like to save the report?

Yes

No

NOTE

Intune提供其他裝置報告欄位，包括應用程式註冊識別碼、Android製造商、型號和安全性修補程式版本，以及iOS/iPadOS 模型。在Intune中，您可以選取 [■****■ > ■■■:iOS/iPadOS■Android] 來存取這些欄位。> 此外，這些參數可協助您設定裝置製造商 (Android) 的 ■■ 裝置型號 (Android和iOS/iPadOS) 的 ■■，以及 ■Android■■■ 設定。

另請參閱

- 管理 iOS/iPadOS 應用程式之間的資料傳輸

- 當您的iOS/iPadOS 應用程式受應用程式保護原則管理時，會發生什麼事

準備好 Windows 資訊保護 Windows 10/11

2022/9/27 •

透過在 Azure AD 中設定 mam 提供者，啟用行動應用程式管理 (MAM) Windows 10/11。在 Azure AD 中設定 MAM 提供者，可讓您在建立新的 Windows 資訊保護使用) 的 (WIP Intune 原則時，定義註冊狀態。註冊狀態可以是 MAM 或 mobile device management (MDM)。

設定 MAM 提供者

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 [所有服務]，然後選擇 [M365 Azure Active Directory] 以切換儀表板。
3. 選取 [Azure Active Directory]。
4. 選擇 [管理] 群組中的 [行動 (MDM 和 MAM)]。
5. 按一下 [Microsoft Intune]。
6. 在 [設定] 窗格上，設定 [還原預設 MAM URLs] 群組中的設定。

MAM 使用者範圍

使用 MAM 自動註冊管理員工 Windows 裝置上的企業資料。MAM 自動註冊會設定為攜帶您自己的裝置案例。

- 無
選取是否無使用者可在 MAM 中登記。
- 一些
選取 [Azure AD 包含將在 MAM 註冊的使用者群組]。
- 全部
選取是否所有使用者都可以在 MAM 中登記。

MAM 使用條款 URL

不支援使用 MAM 使用條款 URL Microsoft Intune。若要套用保護原則，此輸入盒必須保留空白。

MAM 探索 URL

MAM 服務之註冊端點的 URL。註冊端點用於註冊使用 MAM 服務管理的裝置。

MAM 相容性 URL

Microsoft Intune 不支援 MAM 相容性 URL。若要套用保護原則，此輸入盒必須保留空白。

7. 按一下 [儲存]。

後續步驟

[建立 WIP 原則](#)

使用 Intune 建立及部署 Windows 資訊保護 (WIP) 原則

2022/9/27 •

您可以使用 Windows 資訊保護 (WIP) 原則搭配 Windows 10 應用程式來保護應用程式，而不需裝置註冊。

開始之前

新增 WIP 原則時，您必須瞭解一些概念：

允許和免除的應用程式清單

- **受保護的應用程式：**這些應用程式是需要遵循此原則的應用程式。
- **豁免應用程式：**這些應用程式不受此原則限制，可以存取公司資料，而不需任何限制。

應用程式類型

- **建議的應用程式：**預先填入 (的清單，主要是 Microsoft Office) 可讓您輕鬆匯入原則的應用程式。
- **儲存應用程式：**您可以將 Windows 儲存區中的任何應用程式新增至原則。
- **Windows 桌面應用程式：**您可以將任何傳統的 Windows 桌面應用程式新增至原則 (例如，.exe、.dll)

必要條件

您必須先設定 MAM 提供者，才能建立 WIP 原則。深入瞭解 [如何使用 Intune 設定 MAM 提供者](#)。

IMPORTANT

WIP 不支援多重身分識別，一次只能有一個受管理身分識別。如需 WIP 的功能和限制的相關資訊，請參閱[使用 Windows 的資訊保護 \(WIP\) 保護您的企業資料](#)。

此外，您必須具備下列授權和更新：

- [Azure AD Premium](#)授權
- [Windows 建立者更新](#)

新增 WIP 原則

在您的組織中設定好 Intune 之後，您可以建立 WIP 專用原則。

TIP

如需建立 Intune 之 WIP 原則的相關資訊，包括可用設定以及如何加以設定，請參閱在 Windows 安全性文件庫中[使用入口 Microsoft Intune 網站，建立 Windows 資訊保護 \(WIP\) 原則](#)。

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 **應用 > 程式的應用程式保護原則 > 建立原則**。
3. 新增下列值：
 - **名字：**輸入新原則 (必要) 名稱。
 - **描述：**(選用) 輸入描述。

- 平臺：選擇 [Windows 10] 做為您的 WIP 原則所支援的平臺。
 - 註冊狀態：選擇 [無登記] 做為原則的註冊狀態。
4. 選擇 [建立]。原則會建立並顯示在 [應用程式保護原則] 窗格上的表格中。

將建議的應用程式新增至受保護的應用程式清單

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 應用 > 程式的應用程式保護原則。
3. 在 [應用程式保護原則] 窗格中，選擇您要修改的原則。隨即會顯示 [Intune App Protection] 窗格。
4. 從 [Intune App Protection] 窗格中選擇 [受保護的應用程式]。[受保護的應用程式] 窗格隨即開啟，顯示已包含在此 app protection 原則的清單中的所有應用程式。
5. 選取 [新增應用程式]。[新增應用程式] 資訊會顯示已篩選的應用程式清單。窗格上方的清單可讓您變更清單篩選。
6. 選取您要允許存取您公司資料的每個應用程式。
7. 按一下 [確定]。[受保護的應用程式] 窗格會更新，顯示所有選取的應用程式。
8. 按一下 [儲存]。

將 Store 應用程式新增至受保護的應用程式清單

若要新增儲存應用程式

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 應用 > 程式的應用程式保護原則。
3. 在 [應用程式保護原則] 窗格中，選擇您要修改的原則。隨即會顯示 [Intune App Protection] 窗格。
4. 從 [Intune App Protection] 窗格中選擇 [受保護的應用程式]。[受保護的應用程式] 窗格隨即開啟，顯示已包含在此 app protection 原則的清單中的所有應用程式。
5. 選取 [新增應用程式]。[新增應用程式] 資訊會顯示已篩選的應用程式清單。窗格上方的清單可讓您變更清單篩選。
6. 從清單中，選取 [儲存應用程式]。
7. 輸入 [名稱]、[Publisher]、[產品名稱] 及 [動作] 的值。請務必將 動作 值設定為 [允許]，讓應用程式可以存取您的公司資料。
8. 按一下 [確定]。[受保護的應用程式] 窗格會更新，顯示所有選取的應用程式。
9. 按一下 [儲存]。

將桌面應用程式新增至受保護的應用程式清單

新增桌面應用程式

1. 登入 Microsoft 端點管理員系統[管理中心](#)。
2. 選取 應用 > 程式的應用程式保護原則。
3. 在 [應用程式保護原則] 窗格中，選擇您要修改的原則。隨即會顯示 [Intune App Protection] 窗格。
4. 從 [Intune App Protection] 窗格中選擇 [受保護的應用程式]。[受保護的應用程式] 窗格隨即開啟，顯示已包含在此 app protection 原則的清單中的所有應用程式。
5. 選取 [新增應用程式]。[新增應用程式] 資訊會顯示已篩選的應用程式清單。窗格上方的清單可讓您變更清單篩選。
6. 從清單中選取 [桌面應用程式]。
7. 輸入 [名稱]、[Publisher]、[產品名稱]、[最小版本 **]、[**最 小版本] 及 [動作] 的值 請務必將 動作 值設定為 [允許]，讓應用程式可以存取您的公司資料。
8. 按一下 [確定]。[受保護的應用程式] 窗格會更新，顯示所有選取的應用程式。
9. 按一下 [儲存]。

WIP Learning

新增您要使用 WIP 保護的應用程式之後，您必須使用 wip Learning 套用保護模式。

開始之前

WIP Learning 是一種報告，可讓您監視啟用 wip 功能的應用程式和 wip-未知應用程式。未知的應用程式是組織 IT 部門未部署的應用程式。您可以從報告中匯出這些應用程式，並將其新增至您的 WIP 原則，以避免生產力中斷，讓他們在「組塊」模式中強制執行 WIP。

除了查看具有 WIP 功能之應用程式的資訊之外，您還可以查看具有網站共用工作資料之裝置的摘要。您可以使用此資訊，判斷應新增至群組和使用者 WIP 原則的網站。摘要會顯示啟用 WIP 功能的應用程式所存取的網站 URLs。

在使用啟用 WIP 功能的應用程式和 WIP-未知應用程式時，建議您在使用您的受保護的應用程式清單上具有正確應用程式的小型群組進行驗證時，以 **無 訊息**或 **允許覆寫** 的方式開始。完成後，您可以變更為您的最終強制原則，**封鎖**。

保護模式為何？

封鎖

WIP 會尋找不適當的資料共用慣例，並停止使用者完成動作。封鎖的動作可包含跨非公司保護應用程式的共用資訊，以及在組織外的其他人和裝置之間共用公司資料。

允許覆寫

WIP 會尋找不適當的資料共用，並在使用者做為可能不安全的情況時發出警告。不過，此模式可讓使用者覆寫原則及共用資料，將動作記錄到您的審計記錄。

沉默

WIP 會以無訊息的方式執行、記錄不適當的資料共用，而不封鎖任何可能會在 [允許] 覆寫模式中提示您進行員工互動的動作 Unallowed 動作(如應用程式未正確嘗試存取網路資源或 WIP 保護的資料)仍會停止。

不建議使用 0

WIP 已關閉，不會協助保護或審計您的資料。

當您關閉 WIP 後，會嘗試在本機連接的磁片磁碟機上解密任何 WIP 標記的檔案。請注意，如果您開啟 WIP 防護，則不會自動重新套用先前的解密和原則資訊。

新增保護模式

1. 從 **應用程式原則** 窗格中，選擇您的原則的名稱，然後選擇 [**必要設定**]。

![Learning 模式] 窗格的螢幕擷取畫面](./media/windows-information-protection-policy-create/learning-mode-sc1.png)

2. 選取設定，然後選擇 [**儲存**]。

允許 Windows 搜尋索引子搜尋加密的專案

允許或禁止專案的索引。此參數適用於 Windows 搜尋索引子，可控制是否要索引已加密的專案，例如 Windows 資訊保護 (WIP) 保護的檔案。

此應用程式保護原則選項位於 Windows 資訊保護原則的「**高級設定**」中。應用程式保護原則必須設定為 *Windows 10* 平臺，且應用程式原則 **註冊狀態** 必須設定為 **With 註冊名**。

啟用原則時，會將 WIP 受保護的專案編制索引，並將其中繼資料儲存在未加密的位置。中繼資料包含檔路徑和日期等專案。

停用原則時，不會對 WIP 受保護的專案編制索引，也不會顯示在 Cortana 或檔案瀏覽器的結果中。如果裝置上有許多具有 WIP 保護的媒體檔案，則對相片和 Groove 應用程式的效能可能也會有影響。

新增加密的副檔名

除了設定 [允許 Windows 搜尋索引子搜尋加密的專案] 選項之外，您還可以指定副檔名清單。從伺服器郵件區塊複製時，會加密具有這些副檔名的檔案，在 [網路位置] 清單中所定義的公司界限內的 (SMB) 共用。若未指定此原則，則會套用現有的自動加密行為。設定此原則時，只會加密清單中副檔名的檔案。

部署您的 WIP 應用程式保護原則

IMPORTANT

此資訊適用於不含裝置登記的 WIP。

在您建立 WIP 應用程式保護原則之後，您必須使用 MAM 將其部署至您的組織。

1. 在 [應用程式原則] 窗格中，選擇您新建立的應用程式保護原則，然後選擇 [使用者群組] [> 新增使用者群組]。

由 Azure Active Directory 中所有安全性群組組成的使用者群組清單會在 [新增使用者] 群組 窗格中開啟。

2. 選擇您要套用原則的群組，然後選擇 [選取] 以部署原則。

後續步驟

深入瞭解 Windows 資訊保護，請參閱[使用 Windows 資訊保護來保護您的企業資料 \(WIP\)](#)。

如何在 Microsoft Intune 中管理 iOS 應用程式之間的資料傳輸

2022/9/27 •

若要協助保護公司資料，請將檔案傳輸限制為僅限您管理的應用程式。您可以透過下列方式管理 iOS 應用程式：

- 設定應用程式的應用程式保護原則，以保護公司或學校帳戶的組織資料。我們稱之為 *受原則管理的應用程式*。請參閱[Microsoft Intune 受保護的應用程式](#)。
- 透過 iOS 裝置管理來部署和管理應用程式，這需要裝置註冊行動裝置管理 (MDM) 解決方案。您部署的應用程式可以是 *受原則管理的應用程式* 或其他 iOS 受控應用程式。

已註冊 iOS 裝置的「開啟管理」功能可以限制 iOS 受控應用程式之間的檔案傳輸。使用應用程式保護原則設定 *[開啟管理限制]*，此原則會使用 *[開啟/共用]* 篩選值將 *組織資料傳送至其他應用程式* 到受原則管理的應用程式，然後使用 Intune 部署原則。當使用者安裝已部署的應用程式時，您設定的限制會根據指派的原則套用。

使用開啟管理來保護 iOS 應用程式和資料

使用應用程式防護原則搭配 iOS 開啟管理 功能，以下列方式保護公司資料：

- **不受任何 MDM 解決方案管理的裝置：**您可以設定應用程式保護原則設定，以透過 *[開啟]* 或 *[共用擴充功能]* 來控制與其他應用程式共用資料。若要這樣做，請使用 *[開啟/共用]* 篩選值，將 *[將組織資料傳送至其他應用程式]* 設定為 *[受原則管理的應用程式]*。受 *原則管理應用程式* 中的 *[開啟/共用]* 行為只會將其他 *受原則管理的應用程式* 顯示為共用的選項。如需相關資訊，請參閱 [iOS/iPadOS 和 Android 應用程式、資料傳輸和 iOS 共用擴充功能的應用程式防護原則](#)。
- **MDM 解決方案所管理的裝置：**針對註冊 Intune 或協力廠商 MDM 解決方案的裝置，透過應用程式保護原則的應用程式與透過 MDM 部署的其他受控 iOS 應用程式之間的資料共用，是由 Intune 應用程式原則和 iOS 開放式管理 功能所控制。若要確定您使用 MDM 解決方案部署的應用程式也與 Intune 應用程式保護原則相關聯，請設定使用者 UPN 設定，如下一節設定 [使用者 UPN 設定](#) 中所述。若要指定如何允許將資料傳輸至其他 *受原則管理的應用程式*，以及 iOS 受控應用程式，請將 *[將組織資料傳送至其他應用程式]* 設定設定為 *[具有 OS 共用的原則受控應用程式]*。若要指定如何允許應用程式接收來自其他應用程式的資料，請啟用 *[從其他應用程式接收資料]*，然後選擇您慣用的接收資料層級。如需接收和共用應用程式資料的詳細資訊，請參閱 [資料重新配置設定](#)。

設定 Microsoft Intune 或協力廠商 EMM 的使用者 UPN 設定

Intune 或協力廠商 EMM 解決方案所管理的裝置 需要 設定使用者 UPN 設定，才能在將資料傳輸至 iOS 受控應用程式時，識別傳送原則 *受控應用程式* 的已註冊使用者帳戶。UPN 設定適用於您從 Intune 部署的應用程式保護原則。下列程式是如何設定 UPN 設定和產生使用者體驗的一般流程：

1. 在 [Microsoft 端點管理員 系統管理中心](#)，[建立並指派](#) iOS/iPadOS 的應用程式保護原則。根據公司需求設定原則設定，並選取應具有此原則的 iOS 應用程式。
2. 使用下列一般化步驟，部署您想要透過 Intune 或協力廠商 MDM 解決方案管理的應用程式和電子郵件設定檔。範例 1 也涵蓋此體驗。
3. 將具有下列應用程式組態設定的應用程式部署至受控裝置：

key = IntuneMAMUPN, value = [username@company.com](#)

範例: ['IntuneMAMUPN', 'janellecraig@contoso.com']

NOTE

在Intune中，應用程式組態原則註冊類型必須設定為受 。此外，如果應用程式設定為可用，或視需要推送至裝置，則必須從Intune 公司入口網站 (安裝應用程式)。

NOTE

將 IntuneMAMUPN 應用程式組態設定部署至傳送資料的目標受控應用程式。將應用程式組態金鑰新增至接收應用程式是選擇性的。

NOTE

目前，如果相同裝置上有 MDM 註冊的帳戶，則不支援在應用程式上向不同的使用者註冊。

4. 使用Intune或您的協力廠商 MDM 提供者將 **開啟管理** 原則部署到已註冊的裝置。

範例 1: Intune或協力廠商 MDM 主控台中的系統管理員體驗

- 移至 Intune 或協力廠商 MDM 提供者的管理主控台。移至主控台的 區段，其中您會將應用程式組態設定部署至已註冊的iOS裝置。
- 在 [應用程式組態] 區段中，針對將資料傳輸至受控應用程式的每個受原則 **管理應用程式** 輸入下列設定 iOS：

key = IntuneMAMUPN, value = [username@company.com](#)

索引鍵/值組的確切語法可能會根據您的協力廠商 MDM 提供者而有所不同。下表顯示協力廠商 MDM 提供者的範例，以及您應該為索引鍵/值組輸入的確切值。

MDM	IntuneMAMUPN	字串	
Microsoft Intune	IntuneMAMUPN	字串	{{userprincipalname}}
Microsoft Intune	IntuneMAMOID	字串	{{userid}}
VMware AirWatch	IntuneMAMUPN	字串	{UserPrincipalName}
MobileIron	IntuneMAMUPN	字串	\${userUPN}  \${userEmailAddress}
Citrix 端點管理	IntuneMAMUPN	字串	\${user:userprincipalname}
ManageEngine Mobile 裝置管理員	IntuneMAMUPN	字串	%upn%

NOTE

針對 iOS/iPadOS 的Outlook，如果您使用 [使用設定設計工具] 選項應用程式組態原則部署受控裝置，並啟用 []，則會在幕後自動為原則設定設定金鑰 IntuneMAMUPN。如需詳細資訊，請參閱適用於iOS和Android 應用程式組態原則體驗的 [新Outlook - 一般應用程式組態](#) 中的常見問題一節。

範例 2: 使用者體驗

使用 OS 共用從受原則管理的應用程式 共用至其他應用程式

1. 使用者會在已註冊iOS裝置上開啟Microsoft OneDrive應用程式，並登入其工作帳戶。使用者輸入的帳戶必須符合您在Microsoft OneDrive應用程式的應用程式組態設定中指定的帳號 UPN。
2. 登入之後，系統管理員設定的應用程式設定會套用至Microsoft OneDrive中的使用者帳戶。這包括將 [將組織資料傳送至其他應用程式] 設定設定為具有 OS 共用值的原則受控應用程式。
3. 使用者預覽工作檔案，並嘗試透過 Open-in 共用至受控應用程式iOS。
4. 資料傳輸成功，且資料現在受到iOS受控應用程式 中的開啟管理 保護。Intune應用程式不適用於非 受原則管理應用程式的應用程式。

使用**傳入組織資料 從iOS受控應用程式共用 至 受原則管理的應用程式

1. 使用者使用受控電子郵件設定檔，在已註冊iOS裝置上開啟原生郵件。
2. 使用者會開啟從原生郵件到 Microsoft Word 的工作檔附件。
3. 當 Word 應用程式啟動時，會發生兩種體驗之一：
 - a. 當下列狀況下，Intune APP 會保護資料：
 - 使用者已登入其工作帳戶，其符合您在應用程式組態設定中指定的帳號 UPN Microsoft Word應用程式。
 - 系統管理員設定的應用程式設定會套用至Microsoft Word中的使用者帳戶。這包括將 [從其他應用程式接收資料] 設定為 [所有具有傳入組織資料的應用程式] 值。
 - 資料傳輸成功，且檔會標記為應用程式中的工作身分識別。Intune APP 會保護檔的使用者動作。
 - b. 當下列狀況下，Intune APP 不會 保護資料：
 - 使用者 未 登入其工作帳戶。
 - 系統管理員設定的設定 不會 套用至Microsoft Word，因為使用者未登入。
 - 資料傳輸成功，且檔 未 標記為應用程式中的工作身分識別。Intune APP 不會 保護檔的使用者動作，因為它不在使用中。

NOTE

使用者可以使用 Word 新增和使用其個人帳戶。當使用者在工作內容外部使用 Word 時，應用程式防護原則不適用。

驗證協力廠商 EMM 的使用者 UPN 設定

設定使用者 UPN 設定之後，請驗證iOS應用程式接收並遵守Intune應用程式保護原則的能力。

例如，[需要應用程式 PIN] 原則設定很容易測試。當原則設定等於 [需要] 時，使用者應該會看到設定或輸入 PIN 的提示，才能存取公司資料。

首先，[建立應用程式保護原則並指派給iOS應用程式](#)。如需如何測試應用程式保護原則的詳細資訊，請參閱 [驗證應用程式保護原則](#)。

另請參閱

[什麼是Intune應用程式保護原則](#)

複查用戶端應用程式保護記錄

2022/9/27 •

深入瞭解您可以在 app protection 記錄檔中查看的設定。在行動用戶端上啟用 Intune 診斷，存取記錄檔。

啟用及收集記錄的程式因平臺而異：

- **iOS/iPadOS 裝置**-使用 Microsoft Edge iOS/iPadOS 收集記錄檔。如需詳細資訊，請參閱 [使用 Edge for iOS 和 Android 存取受管理的應用程式記錄檔](#)。
- **Windows 10/11 裝置**-使用 *MDMDiag* 和事件記錄。請參閱 Windows 用戶端管理內容中的 [Windows 10 診斷 MDM 失敗](#)，以及 [博客疑難排解 Windows 10 Intune 原則失敗](#)。
- **android 裝置**-使用適用於 android 的 Microsoft Edge 來收集記錄檔。如需詳細資訊，請參閱 [使用 Edge for iOS 和 Android 存取受管理的應用程式記錄檔](#)。

NOTE

在 Android 完全受管理的裝置上，在某些情況下，Intune 公司入口網站應用程式可能會顯示在 [所有應用程式] 底下。當應用程式保護原則相關聯的應用程式未安裝或尚未啟動時，可能會發生這種情況。

下表列出記錄檔中所記錄的應用程式防護原則設定名稱及支援的值。此外，每個設定會識別 Microsoft 端點管理員入口網站內找到的原則設定。如需每個設定的詳細資訊，請參閱 Microsoft Intune 中的 [iOS/iPadOS 應用程式保護原則設定](#) 和 [Android 應用程式保護原則設定](#)。

iOS/iPadOS 應用程式防護原則設定

名稱	值	MICROSOFT 識別碼
AccessRecheckOfflineTimeout	x 分鐘	■: 條件式發佈 ■: 具有動作區塊存取的離線寬限期 (分鐘)
AccessRecheckOnlineTimeout	x 分鐘	■: 存取需求 ■: 在 (分鐘) 的非活動狀態之後重新檢查存取需求
AllowedIOSModelsElseBlock	x 個字元	■: 條件式發佈 ■: 裝置模型 (s) 具有動作允許指定 (封鎖非特定)
AllowedIOSModelsElseWipe	x 個字元	■: 條件式發佈 ■: 裝置模型 (s) 具有動作允許指定 (清除非特定)
AppActionIfUnableToAuthenticateUser	0 = 封鎖存取 1 = 需要擦除資料	■: 條件式發佈 ■: 停用帳戶
AppPinDisabled	0 = 需要 1 = 非必要	■: 存取需求 ■: 裝置 pin 碼設定時的應用程式 PIN 碼

名稱	說明	MICROSOFT 說明
AppSharingFromLevel	0 = 無 1 = 原則管理的應用程式 2 = 所有應用程式	■: 資料保護 ■: 從其他應用程式接收資料
AppSharingToLevel	0 = 無 1 = 原則管理的應用程式 2 = 所有應用程式	■: 資料保護 ■: 將組織資料傳送至其他應用程式
AuthenticationEnabled	0 = 非必要 1 = 需要	■: 存取需求 ■: 存取的工作單位或學校帳號憑證
ClipboardCharacterExceptionLength	x 個字元	■: 資料保護 ■: 剪下及複製任何應用程式的字元限制
ClipboardEncryptionEnabled	0 = 停用 1 = 啟用	此設定沒有管理控制權。
ClipboardSharingLevel	0 = 封鎖 1 = 原則管理的應用程式 2 = 具有貼上的原則管理應用程式 3 = 任何應用程式	■: 資料保護 ■: 限制其他應用程式之間的剪下、複製和貼上
ContactSyncDisabled	0 = 允許 1 = 封鎖	■: 資料保護 ■: 使用原生連絡人應用程式的 Sync 應用程式
DataBackupDisabled	0 = 允許 1 = 封鎖	■: 資料保護 ■: 防止備份
DeviceComplianceEnabled	0 = False 1 = True	■: 條件式發佈 ■: 已越獄/有根的裝置
DeviceComplianceFailureAction	0 = 封鎖存取 1 = 擦除資料	■: 條件式發佈 ■: 已越獄/有根的裝置
DialerRestrictionLevel	0 = 無, 請勿在應用程式之間傳輸此資料 1 = 特定撥號器應用程式 3 = 任何撥號器應用程式	■: 資料保護 ■: 將電信資料傳輸至
DictationBlocked	0 = 允許 1 = 封鎖	此設定沒有管理控制權。
DisableShareSense	不適用	N/A: Intune 服務未主動使用。
EnableOpenInFilter	0 = 停用 1 = 啟用	■: 資料保護 ■: 將組織資料傳送至其他應用程式 > 原則管理的應用程式與開啟中/共用篩選
FaceIDEnabled	0 = 封鎖 1 = 允許	■: 存取需求 ■: 面孔識別碼, 而不是 PIN 存取 (iOS 11 + /iPadOS)

名稱	說明	MICROSOFT 說明
FileEncryptionLevel	0 = 當裝置鎖定時 1 = 何時鎖定裝置, 且有開啟的檔案 2 = 在裝置重新開機後 3 = 使用裝置設定	■: 資料保護 ■: 加密組織資料
FileSharingSaveAsDisabled	0 = 允許 1 = 封鎖	■: 資料保護 ■: 儲存組織資料的副本
IntuneIdentityUPN	Intune MAM 使用者的 UPN	不適用
ManagedBrowserRequired	0 = False 1 = True	■: 資料保護 ■: 限制與其他應用程式的 web 內容傳輸
ManagedLocations	值, 代表應用程式可儲存資料的受管理儲存位置數目。 1 = OneDrive 2 = SharePoint 3 = OneDrive 和 SharePoint 32 = Local 儲存體 33 = Local 儲存體 & OneDrive 34 = Local 儲存體 & SharePoint 35 = Local 儲存體、OneDrive 及 SharePoint	■: 資料保護 ■: 允許使用者將副本儲存到選取的服務
ManagedUniversalLinks	通用連結清單, 可讓您在對應的受管理應用程式中開啟資料	■: 資料保護 ■: 選取 managed 通用連結
MaxPinRetryExceededAction	0 = 重設 PIN 碼 1 = 擦除資料	■: 條件式發佈 ■: PIN 碼嘗試次數上限
MaxOsVersion	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 具有動作區塊存取的最大作業系統版本
MaxOsVersionWarning	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 具有動作警告的最大作業系統版本
MaxOsVersionWipe	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 含動作的最大作業系統版本清除資料
MinAppVersion	"0.0" = 無最低應用程式版本 其他任何專案 = 最低應用程式版本	■: 條件式發佈 ■: 具有動作區塊存取的最小應用程式版本
MinAppVersionWarning	"0.0" = 無最低應用程式版本。 其他任何專案 = 最低應用程式版本	■: 條件式發佈 ■: 具有動作警告的最小應用程式版本
MinAppVersionWipe	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作的最小應用程式版本清除資料
MinOsVersion	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作區塊存取的最小作業系統版本

名稱	說明	MICROSOFT 建議值
MinOsVersionWarning	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作警告的最小作業系統版本
MinOsVersionWipe	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 含動作的最小作業系統版本清除資料
MinSDKVersion	"0.0" = 無最低的 SDK 版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作區塊存取的最小 SDK 版本
MinSDKVersionWipe	"0.0" = 無最低的 SDK 版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作區塊存取的最小 SDK 版本
MinimumRequiredDeviceThreatProtectionLevel	0 = 未設定 1 = 安全 2 = 低 3 = 中速 4 = 高	■: 條件式發佈 ■: 允許的最大裝置威脅層級
MobileThreatDefenseRemediationAction	0 = 封鎖存取 1 = 擦除資料	■: 存取需求 ■: 允許的最大裝置威脅層級動作)
NonBioPassTimeOutRequired	0 = 非必要 1 = 需要	■: 存取需求 ■: 以 PIN 碼超時後覆寫觸控識別碼
NonBioPassTimeOut	x 分鐘	■: 存取需求 ■: 以 PIN 碼超時 > 超時, 覆寫觸控識別碼超時 (分鐘非使用中)
NotificationRestriction	0 = 允許 1 = 封鎖組織資料 2 = 封鎖	■: 資料保護 ■: Org data 通知
OpenDataFromManagedLocations	值, 代表應用程式可儲存資料的受管理儲存位置數目。 1 = OneDrive 2 = SharePoint 3 = OneDrive 和 SharePoint 4 = 相機 5 = OneDrive & 相機 6 = SharePoint & 相機 7 = 相機、OneDrive 和 SharePoint	■: 資料保護 ■: 允許使用者開啟選取服務中的資料
OpenDataIntoOrgDocumentsBlocked	0 = 允許 1 = 封鎖	■: 資料保護 ■: 開啟組織檔中的資料
OfflineWipeInterval	x 天	■: 此設定沒有系統管理控制。
PINCharacterType	0 = 密碼 1 = 數值	■: 存取需求 ■: Pin 類型
PINEnabled	0 = 非必要 1 = 需要	■: 存取需求 ■: 存取權的 PIN 碼
PINExpiryDays	x 個字元	■: 存取需求 ■: 在天數 > 天數後重設 PIN 碼的數目

名稱	說明	MICROSOFT 說明
PINMinLength	x 個字元	■: 存取需求 ■: 選取最小 PIN 碼長度
PINNumRetry	x 次嘗試	■: 條件式發佈 ■: PIN 碼嘗試次數上限
PrintingBlocked	0 = 允許 1 = 封鎖	■: 資料保護 ■: 列印組織資料
ProtectAllIncomingUnknownSourceData	不適用	■: Intune 服務未主動使用。
ProtectManagedOpenInData	0 = False 1 = True	■: 資料保護 ■: 若為 true, 將組織資料傳送至其他應用程式, 則會設定為使用開啟/共用篩選的原則管理應用程式。請注意, 當啟用具有作業系統共用的原則管理應用程式時, 也可以設定為 1。
ProtocolExclusions	應用程式 URL 通訊協定架構的清單, 可讓資料在對應的未受管理的應用程式資料中開啟	■: 資料保護 ■: 選取要免除的應用程式
RequireFileEncryption	不適用	■: Intune 服務未主動使用。
SimplePINAllowed	0 = 封鎖 1 = 允許	■: 存取需求 ■: 簡易 PIN
SpecificDialerProtocol	從受管理的應用程式通話所用之特定撥號器的 URL 通訊協定配置	■: 資料保護 ■: 撥號器應用程式 URL 配置
ThirdPartyKeyboardsBlocked	0 = 允許 1 = 封鎖	■: 資料保護 ■: 協力廠商鍵盤
TouchIDEnabled	0 = 封鎖 1 = 允許	■: 存取需求 ■: 觸控識別碼, 而不是使用 PIN 存取 (iOS 8 +/iPadOS)
UniversalLinkExclusions	通用連結清單, 可讓您在對應的非管理應用程式中開啟資料	■: 資料保護 ■: 選取要免除的通用連結
UnmanagedBrowserProtocol	用於查看受管理網頁連結之非管理瀏覽器的 URL 通訊協定配置	■: 資料保護 ■: 限制與其他應用程式的 web 內容傳輸

Android 應用程式防護原則設定

名稱	說明	MICROSOFT 說明
AccessRecheckOfflineTimeout	x 分鐘	■: 條件式發佈 ■: 具有動作區塊存取的離線寬限期 (分鐘)

名稱	說明	MICROSOFT 說明
AccessRecheckOnlineTimeout	x 分鐘	■: 存取需求 ■: 在 (分鐘的非活動狀態之後重新檢查存取需求)
AllowedAndroidManufacturersElseBlock	若未設定, 則為空, 否則為允許的製造商清單	■: 條件式發佈 ■: 具有動作的裝置製造商指定的 (區塊未指定)
AllowedAndroidManufacturersElseWipe	若未設定, 則為空, 否則為允許的製造商清單	■: 條件式發佈 ■: 具有動作的裝置生產商允許指定 (清除非指定的)
AllowedAndroidModelsElseBlock	若未設定, 則為空, 否則為允許的模型清單	此設定沒有管理控制權。
AllowedAndroidModelsElseWipe	若未設定, 則為空, 否則為允許的模型清單	此設定沒有管理控制權。
AndroidSafetyNetDeviceAttestationEnforcement	NOT_REQUIRED = 未設定 BASIC_INTEGRITY = 基本完整性 BASIC_INTEGRITY_AND_DEVICE_CERTIFICATION = 基本的完整性及驗證裝置	■: 條件式發佈 ■: SafetyNet 裝置認證
AndroidSafetyNetDeviceAttestationFailedAction	BLOCK = 封鎖存取 警告 = 警告 WIPE_DATA = 清除資料	■: 條件式發佈 ■: SafetyNet 裝置認證
AndroidSafetyNetVerifyAppsEnforcementType	NOT_REQUIRED = 未設定 REQUIRE_ENABLED = 設定	■: 條件式發佈 ■: 需要在應用程式上進行威脅掃描
AndroidSafetyNetVerifyAppsFailedAction	BLOCK = 封鎖存取 警告 = 警告	■: 條件式發佈 ■: 需要在應用程式上進行威脅掃描
AppActionIfUnableToAuthenticateUser	NONE = 未設定 BLOCK = 封鎖存取 WIPE_DATA = 清除應用程式	■: 條件式發佈 ■: 停用帳戶
AppPinDisabled	true = 需要 false = 非必要	■: 存取需求 ■: 裝置 pin 碼設定時的應用程式 PIN 碼
ApprovedKeyboards	IDs 必要的核准鍵盤捆綁清單	■: 資料保護 ■: 選取要核准的鍵盤
AppSharingFromLevel	封鎖 = 無 MANAGED = 原則管理的應用程式 無限制 = 所有應用程式	■: 資料保護 ■: 從其他應用程式接收資料
AppSharingToLevel	封鎖 = 無 MANAGED = 原則管理的應用程式 無限制 = 所有應用程式	■: 資料保護 ■: 將組織資料傳送至其他應用程式
AuthenticationEnabled	false = 非必要 true = 需要	■: 存取需求 ■: 存取的工作單位或學校帳號憑證

名稱	說明	MICROSOFT 說明
BiometricIdEnabled	0 = 封鎖 1 = 允許	■:存取需求 ■:生物識別的生物特徵, 而不是 PIN 存取權
BlockAfterCompanyPortalUpdateDeferralInDays	x 天	■:條件式發佈 ■:最大公司入口網站版本壽命 (天數)
BlockClockStatusWithGracePeriod	不適用	■: Intune 服務未主動使用。
BlockScreenCapture	false = 允許 true = 封鎖	■:資料保護 ■:螢幕截圖和 Google Assistant
ClipboardCharacterExceptionLength	x 個字元	■:資料保護 ■:剪下及複製任何應用程式的字元限制
ClipboardSharingLevel	封鎖 = 封鎖 MANAGED = 原則管理的應用程式 MANAGED_PASTE_IN = 具有貼上的原則管理應用程式 非管理 = 任何應用程式	■:資料保護 ■:限制其他應用程式之間的剪下、複製和貼上
ConditionalEncryptionEnabled	false = 需要 true = 非必要	■:資料保護 ■:加密已註冊裝置上的組織資料
ConnectToVPNOnLaunch	不適用	■: Intune 服務未主動使用。
ContactSyncDisabled	false = 允許 true = 封鎖	■:資料保護 ■:使用原生連絡人應用程式的 Sync 應用程式
DataBackupDisabled	false = 允許 true = 封鎖	■:資料保護 ■:防止備份
DeviceComplianceEnabled	false = False true = True	■:條件式發佈 ■:已越獄/有根的裝置
DeviceComplianceFailureAction	BLOCK = 封鎖存取 WIPE_DATA = 清除資料	■:條件式發佈 ■:已越獄/有根的裝置
DialerRestrictionLevel	0 = 無, 請勿在應用程式之間傳輸此資料 1 = 特定撥號器應用程式 2 = 任何原則管理的撥號器應用程式 3 = 任何撥號器應用程式	■:資料保護 ■:將電信資料傳輸至
DictationBlocked	false = 允許 true = 封鎖	此設定沒有管理控制權。
FileEncryptionKeyLength	128 256	此設定沒有管理控制權。
FileSharingSaveAsDisabled	false = 允許 true = 封鎖	■:資料保護 ■:儲存組織資料的副本

名稱	說明	MICROSOFT 說明
IntuneMAMPolicyVersion	版本號碼	不適用
isManaged	真假	不適用
KeyboardsRestricted	true = 必要 false = 非必要	■: 資料保護 ■: 核准的鍵盤
ManagedBrowserRequired	true = Microsoft Edge 或未受管理的瀏覽器 false = 任何應用程式	■: 資料保護 ■: 將 web 內容傳輸限制為其他應用程式應用程式。
ManagedLocations	一個值, 代表應用程式可以儲存資料的受管理儲存位置數目 (以分號分隔)。 ONEDRIVE_FOR_BUSINESS SHAREPOINT 當地	■: 資料保護 ■: 允許使用者將副本儲存到選取的服務
MaxPinRetryExceededAction	RESET_PIN = 重設 PIN 碼 WIPE_DATA = 清除資料	■: 條件式發佈 ■: PIN 碼嘗試次數上限
MaxOsVersion	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 具有動作區塊存取的最大作業系統版本
MaxOsVersionWarning	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 具有動作警告的最大作業系統版本
MaxOsVersionWipe	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 含動作的最大作業系統版本清除資料
MinAppVersion	"0.0" = 無最低應用程式版本 其他任何專案 = 最低應用程式版本	■: 條件式發佈 ■: 具有動作區塊存取的最小應用程式版本
MinAppVersionWarning	"0.0" = 無最低應用程式版本。 其他任何專案 = 最低應用程式版本	■: 條件式發佈 ■: 具有動作警告的最小應用程式版本
MinAppVersionWipe	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作的最小應用程式版本清除資料
MinOsVersion	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作區塊存取的最小作業系統版本
MinOsVersionWarning	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作警告的最小作業系統版本
MinOsVersionWipe	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 含動作的最小作業系統版本清除資料
MinPatchVersion	"0000-00-00" = 無最低的修補程式版本 其他任何專案 = 最低修補程式版本	■: 條件式發佈 ■: 具有 action 封鎖存取的修補程式版本最小

名稱	說明	MICROSOFT 策略名稱
PINCharacterType	密碼 = 密碼 數值 = 數值	■: 存取需求 ■: Pin 類型
PINEnabled	false = 非必要 true = 需要	■: 存取需求 ■: 存取權的 PIN 碼
PINExpiryDays	x 個字元	■: 存取需求 ■: 在天數 > 天數後重設 PIN 碼的數目
PINMinLength	x 個字元	■: 存取需求 ■: 選取最小 PIN 碼長度
PINNumRetry	x 次嘗試	■: 條件式發佈 ■: PIN 碼嘗試次數上限
PackageExclusions	若未設定任何束 IDs, 則為空, 否則會以分號分隔 IDs	■: 資料保護 ■: 選取要免除的應用程式
PinHistoryLength	要維護的 x PIN 碼值	■: 存取需求 ■: 選取要維護的先前 PIN 碼值數目
PolicyCount	number	不適用
PrintingBlocked	false = 允許 true = 封鎖	■: 資料保護 ■: 列印組織資料
RequireDeviceLock	true = 必要 false = 非必要	■: 條件式發佈 ■: 需要鎖定裝置
RequireDeviceLockEnforcementType	BLOCK = 封鎖存取 WIPE_DATA = 需要擦除	■: 條件式發佈 ■: 需要鎖定裝置
RequireFileEncryption	false = 非必要 true = 需要	■: 資料保護 ■: 加密組織資料
SimplePINAllowed	false = 封鎖 true = 允許	■: 存取需求 ■: 簡易 PIN
SpecificDialerDisplayName	撥號器應用程式名稱	■: 資料保護 ■: 撥號器應用程式名稱
SpecificDialerPackageID	撥號器應用程式束識別碼	■: 資料保護 ■: 撥號器應用程式套件識別碼
TouchIDEnabled	false = 封鎖 true = 允許	■: 存取需求 ■: 指紋, 而不是使用 PIN 存取 (Android 9.0 +)
UnmanagedBrowserDisplayName	未受管理的網頁瀏覽器顯示名稱	■: 資料保護 ■: 非受管理的瀏覽器名稱
UnmanagedBrowserPackageID	非管理網頁瀏覽器套件識別碼	■: 資料保護 ■: 非管理的瀏覽器識別碼

名稱	說明	MICROSOFT 建議值
UserStatusPollInterval	不適用	■: Intune 服務未主動使用。
UserStatusTimeoutInSeconds	不適用	■: Intune 服務未主動使用。

後續步驟

- 若要深入瞭解應用程式保護原則，請參閱 [什麼是應用程式保護原則？](#)
- Intune 提供許多工具，協助您疑難排解環境中的問題。如需詳細資訊，請參閱 [使用疑難排解入口網站協助使用者](#)。

Office 應用程式的原則

2022/9/27 •

Intune 提供專用於 Microsoft Office 應用程式的原則。您可以針對連接至 Microsoft 365 服務的 Office 行動應用程式，選取建立行動應用程式管理原則的特定選項。Office 應用程式有許多原則，您可以新增至 Microsoft Intune 並套用至使用者群組。

只是一些 Office 應用程式原則的範例包括下列各項：

- Microsoft Word: *關閉從 Outlook 開啟之附件的受保護的檢視*
- Microsoft Visio: *封鎖從網際網路 Office 檔案中執行的宏*
- Microsoft Project: *允許網路上的信任位置*
- Microsoft Publisher: *Publisher 自動化安全性層級*
- Microsoft PowerPoint: *關閉從 Outlook 開啟之附件的受保護的檢視*

NOTE

當您選取設定每個特定的應用程式原則時，會提供其他原則的詳細資料。您可以篩選 Office 原則清單，以快速選取建議的  原則。

您也可以 Outlook 為 iOS/iPadOS 建立 Intune 應用程式保護原則，以及使用混合式新式驗證來啟用 Android，以保護 Exchange 內部部署信箱的存取權。使用此功能之前，必須符合使用 Office 雲端原則服務的需求。連接至內部部署 Exchange 或 SharePoint 服務的其他應用程式不支援應用程式防護原則。如需相關資訊，請參閱[Office 雲端原則服務 Microsoft 365 Apps 企業版的概述](#)。

必要條件

您必須符合對 Office 應用程式使用原則的需求。如需詳細資訊，請參閱[使用 Office 雲端原則服務的需求](#)。

若要新增 Office 應用程式原則

在您設定組織的 Intune 後，您可以建立 Office 應用程式原則。

1. 登入 [Microsoft 端點管理員系統管理中心](#)。
2. 選取 **Office 應用程式 > 建立 的 應用程式 > 原則**。
3. 新增下列值：
 - **名字**：輸入新原則 (必要) 名稱。
 - **描述**：(選用) 輸入描述。
 - **選取類型**：選取套用此原則設定的方式。
 - **選取群組**：選取此原則設定的群組。
 - **設定原則**：選取您要套用的 Office 原則。您可以根據原則、平臺、應用程式、建議和狀態，排序提供的清單。
4. 選取 **[建立]**。原則會建立並顯示在 **[原則 設定]** 窗格上的表格中。

TIP

[ 設定] 窗格會提供每個原則的 。

其他資訊

- [Microsoft 365 Apps 企業版 Office cloud policy service 的概覽](#)
- [使用原則設定來管理 Microsoft 365 Apps 企業版的隱私權控制](#)
- [使用喜好設定來管理 Mac 版 Office 的隱私權控制](#)
- [使用喜好設定來管理 iOS 裝置上的 Office 的隱私權控制](#)
- [使用原則設定來管理 Android 裝置上的 Office 隱私權控制](#)

後續步驟

- [使用 Microsoft Intune 監視應用程式資訊和工作分派](#)

使用疑難排解入口網站協助您公司的使用者。

2022/9/27 •

疑難排解入口網站可讓協助服務台操作員和 Intune 系統管理員查看使用者資訊以處理使用者的協助要求。包含服務台的組織可以將 **服務台操作員** 指派給使用者群組。服務台操作員角色可以使用 **疑難排解** 窗格。

疑難排解 窗格也會顯示使用者登記問題。有關問題的詳細資料及建議的修復步驟，可協助系統管理員和問訊台操作員進行問題的疑難排解。未捕獲某些登記問題，有些錯誤可能沒有修正建議。

如需新增服務台操作員角色的步驟，請參閱 [以角色為基礎的管理控制 \(RBAC\) With Intune](#)

當使用者使用 Intune 的技術問題來支援時，問訊台操作員會輸入使用者的名稱。Intune 會顯示有用的資料，可協助解決許多第1層問題，包括：

- 使用者狀態
- 作業
- 規範問題
- 裝置無回應
- 裝置沒有取得 VPN 或 Wi-Fi 設定
- 應用程式安裝失敗

若要查看疑難排解詳細資料

在 [疑難排解] 窗格中，選擇 [**選取使用者**] 以查看使用者資訊。使用者資訊可協助您瞭解使用者及其裝置的目前狀態。

1. 登入 [Intune](#)。
2. 在 [Intune] 窗格中，選擇 [**疑難排解**]。
3. 按一下 [**選取**]，以選取要疑難排解的使用者。
4. 輸入名稱或電子郵件地址，以選取使用者。按一下 [**選取**]。使用者的疑難排解資訊會顯示在 [疑難排解] 窗格中。下表說明此資訊。

NOTE

您也可以將瀏覽器指向：，以存取  窗格 <https://aka.ms/intunetroubleshooting>。

疑難排解儀表板的區域

您可以使用 **疑難排解** 窗格來複查使用者資訊。

The screenshot shows the Microsoft Intune user management interface for a user named 'IW User 4'. The interface includes a top header with the user's name and account status (Active). A sidebar on the left contains options for 'Intune license' and 'GROUP MEMBERSHIP'. The main content area displays 'ASSIGNMENTS' for compliance policies and a list of 'DEVICES' managed by the user.

☐☐	☐☐	☐☐
1.	帳戶狀態	顯示 ■ Intune 租使用者狀態為使用中或 ■ 使用中。
2.	使用者選擇	目前選取之使用者的名稱。按一下 [■ ■] 以選擇新的使用者。
3.	使用者狀態	顯示使用者的 Intune 授權、裝置數目及每個裝置符合性的狀態。
4.	使用者資訊	使用清單來選取要查看窗格中的詳細資料。 您也可以選取： • 用戶端應用程式 • 合規性原則 • 配置原則 • 應用程式防護原則 • 註冊限制
5.	群組成員資格	顯示選取之使用者隸屬的目前群組。

註冊失敗參考

[註冊失敗] 表格會列出失敗的註冊嘗試。下表所列的裝置可能會在另一次嘗試期間成功註冊。可能未列出某些失敗嘗試。所有失敗都無法使用緩解資訊。

☐☐☐	☐☐
註冊開始	使用者第一次開始註冊的開始時間。
作業系統	裝置的作業系統。
作業系統版本	裝置的作業系統版本。
失敗	失敗的原因。

失敗詳細資料

當您選擇 [失敗] 列時，會提供更多詳細資料。

❏	❏
失敗詳細資料	失敗的詳細說明。
潛在 remediations	建議的解決錯誤的步驟。某些失敗可能沒有 remediations。
資源 (選用)	在入口網站中進一步閱讀或區域的連結，以採取動作。

註冊錯誤

❏	❏❏❏
iOS/iPadOS 超時或失敗	在裝置與 Intune 之間的超時，因為使用者花費的時間太長，所以無法完成註冊。
找不到或未獲授權的使用者	使用者缺少授權或已從服務中移除。
已註冊的裝置	有人企圖使用公司入口網站在其他使用者仍已註冊的裝置上登錄裝置。
無法架至 Intune	當 Intune mobile device management (MDM) 授權未設定時，嘗試進行註冊。
註冊授權失敗	使用舊版本的公司入口網站嘗試註冊。
不支援的裝置	裝置不符合 Intune 註冊的最低需求。
未滿足註冊限制	因為系統管理員已設定註冊限制，所以已封鎖此註冊。
裝置版本太低	管理員已設定需要較高裝置版本的註冊限制。
裝置版本太高	管理員已設定註冊限制，需要較低的裝置版本。
裝置無法註冊為個人	管理員已設定註冊限制，以封鎖個人註冊，但未將失敗的裝置預先定義為公司。
封鎖裝置平臺	管理員已設定可封鎖此裝置平臺的註冊限制。
大量權杖已到期	布建套件中的大量權杖已過期。
找不到 Autopilot 裝置或詳細資料	嘗試註冊時，未找到 Autopilot 裝置。
找不到或未指派 Autopilot 設定檔	裝置沒有主動 Autopilot 設定檔。
意外的 Autopilot 註冊方法	裝置嘗試使用不允許的方法進行註冊。
移除 Autopilot 裝置	已從 Autopilot 為此帳戶移除嘗試註冊的裝置。
已達到裝置 cap	因為系統管理員已設定裝置限制限制，所以已封鎖此註冊。
Apple 上架	由於 Intune 中的 Apple MDM push 憑證遺失或過期，所以已封鎖所有 iOS/iPadOS 裝置。

❗	❗❗❗
不 preregistered 裝置	裝置未預先註冊成公司，且所有個人註冊遭到系統管理員封鎖。
不支援的功能	使用者可能嘗試透過與 Intune 設定不相容的方法來註冊。

從行動裝置收集可用資料

當疑難排解使用者的裝置問題時，請使用下列資源協助收集裝置資料：

- [將 iOS/iPadOS 註冊錯誤傳送給您的 IT 管理員](#)
- [協助您的公司支援詳細記錄中的修復裝置問題](#)
- [使用 USB 纜線將 Android 記錄傳送至公司支援](#)
- [使用電子郵件將 Android 診斷資料記錄傳送給 IT 管理員](#)
- [將 Android 註冊錯誤傳送給您的 IT 系統管理員](#)

後續步驟

您可以深入瞭解以角色為基礎的管理控制 (RBAC)，以定義組織裝置中的角色、行動應用程式管理、資料保護工作。如需詳細資訊，請參閱 [使用 Intune \(RBAC\) 的角色型管理控制](#)。

深入瞭解 Microsoft Intune 中的任何已知問題。如需詳細資訊，請參閱[Microsoft Intune 中的已知問題](#)。

瞭解如何在需要時建立支援票證 a 取得協助。[取得支援](#)。

複查用戶端應用程式保護記錄

2022/9/27 •

深入瞭解您可以在 app protection 記錄檔中查看的設定。在行動用戶端上啟用 Intune 診斷，存取記錄檔。

啟用及收集記錄的程式因平臺而異：

- **iOS/iPadOS 裝置**-使用 Microsoft Edge iOS/iPadOS 收集記錄檔。如需詳細資訊，請參閱 [使用 Edge for iOS 和 Android 存取受管理的應用程式記錄檔](#)。
- **Windows 10/11 裝置**-使用 *MDMDiag* 和事件記錄。請參閱 Windows 用戶端管理內容中的 [Windows 10 診斷 MDM 失敗](#)，以及 [博客疑難排解 Windows 10 Intune 原則失敗](#)。
- **android 裝置**-使用適用於 android 的 Microsoft Edge 來收集記錄檔。如需詳細資訊，請參閱 [使用 Edge for iOS 和 Android 存取受管理的應用程式記錄檔](#)。

NOTE

在 Android 完全受管理的裝置上，在某些情況下，Intune 公司入口網站應用程式可能會顯示在 [所有應用程式] 底下。當應用程式保護原則相關聯的應用程式未安裝或尚未啟動時，可能會發生這種情況。

下表列出記錄檔中所記錄的應用程式防護原則設定名稱及支援的值。此外，每個設定會識別 Microsoft 端點管理員入口網站內找到的原則設定。如需每個設定的詳細資訊，請參閱 Microsoft Intune 中的 [iOS/iPadOS 應用程式保護原則設定](#) 和 [Android 應用程式保護原則設定](#)。

iOS/iPadOS 應用程式防護原則設定

名稱	值	MICROSOFT 識別碼
AccessRecheckOfflineTimeout	x 分鐘	■: 條件式發佈 ■: 具有動作區塊存取的離線寬限期 (分鐘)
AccessRecheckOnlineTimeout	x 分鐘	■: 存取需求 ■: 在 (分鐘) 的非活動狀態之後重新檢查存取需求
AllowedIOSModelsElseBlock	x 個字元	■: 條件式發佈 ■: 裝置模型 (s) 具有動作允許指定 (封鎖非特定)
AllowedIOSModelsElseWipe	x 個字元	■: 條件式發佈 ■: 裝置模型 (s) 具有動作允許指定 (清除非特定)
AppActionIfUnableToAuthenticateUser	0 = 封鎖存取 1 = 需要擦除資料	■: 條件式發佈 ■: 停用帳戶
AppPinDisabled	0 = 需要 1 = 非必要	■: 存取需求 ■: 裝置 pin 碼設定時的應用程式 PIN 碼

名稱	說明	MICROSOFT 說明
AppSharingFromLevel	0 = 無 1 = 原則管理的應用程式 2 = 所有應用程式	■: 資料保護 ■: 從其他應用程式接收資料
AppSharingToLevel	0 = 無 1 = 原則管理的應用程式 2 = 所有應用程式	■: 資料保護 ■: 將組織資料傳送至其他應用程式
AuthenticationEnabled	0 = 非必要 1 = 需要	■: 存取需求 ■: 存取的工作單位或學校帳號憑證
ClipboardCharacterExceptionLength	x 個字元	■: 資料保護 ■: 剪下及複製任何應用程式的字元限制
ClipboardEncryptionEnabled	0 = 停用 1 = 啟用	此設定沒有管理控制權。
ClipboardSharingLevel	0 = 封鎖 1 = 原則管理的應用程式 2 = 具有貼上的原則管理應用程式 3 = 任何應用程式	■: 資料保護 ■: 限制其他應用程式之間的剪下、複製和貼上
ContactSyncDisabled	0 = 允許 1 = 封鎖	■: 資料保護 ■: 使用原生連絡人應用程式的 Sync 應用程式
DataBackupDisabled	0 = 允許 1 = 封鎖	■: 資料保護 ■: 防止備份
DeviceComplianceEnabled	0 = False 1 = True	■: 條件式發佈 ■: 已越獄/有根的裝置
DeviceComplianceFailureAction	0 = 封鎖存取 1 = 擦除資料	■: 條件式發佈 ■: 已越獄/有根的裝置
DialerRestrictionLevel	0 = 無, 請勿在應用程式之間傳輸此資料 1 = 特定撥號器應用程式 3 = 任何撥號器應用程式	■: 資料保護 ■: 將電信資料傳輸至
DictationBlocked	0 = 允許 1 = 封鎖	此設定沒有管理控制權。
DisableShareSense	不適用	N/A: Intune 服務未主動使用。
EnableOpenInFilter	0 = 停用 1 = 啟用	■: 資料保護 ■: 將組織資料傳送至其他應用程式 > 原則管理的應用程式與開啟中/共用篩選
FaceIDEnabled	0 = 封鎖 1 = 允許	■: 存取需求 ■: 面孔識別碼, 而不是 PIN 存取 (iOS 11 + /iPadOS)

名稱	說明	MICROSOFT 說明
FileEncryptionLevel	0 = 當裝置鎖定時 1 = 何時鎖定裝置, 且有開啟的檔案 2 = 在裝置重新開機後 3 = 使用裝置設定	■: 資料保護 ■: 加密組織資料
FileSharingSaveAsDisabled	0 = 允許 1 = 封鎖	■: 資料保護 ■: 儲存組織資料的副本
IntuneIdentityUPN	Intune MAM 使用者的 UPN	不適用
ManagedBrowserRequired	0 = False 1 = True	■: 資料保護 ■: 限制與其他應用程式的 web 內容傳輸
ManagedLocations	值, 代表應用程式可儲存資料的受管理儲存位置數目。 1 = OneDrive 2 = SharePoint 3 = OneDrive 和 SharePoint 32 = Local 儲存體 33 = Local 儲存體 & OneDrive 34 = Local 儲存體 & SharePoint 35 = Local 儲存體、OneDrive 及 SharePoint	■: 資料保護 ■: 允許使用者將副本儲存到選取的服務
ManagedUniversalLinks	通用連結清單, 可讓您在對應的受管理應用程式中開啟資料	■: 資料保護 ■: 選取 managed 通用連結
MaxPinRetryExceededAction	0 = 重設 PIN 碼 1 = 擦除資料	■: 條件式發佈 ■: PIN 碼嘗試次數上限
MaxOsVersion	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 具有動作區塊存取的最大作業系統版本
MaxOsVersionWarning	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 具有動作警告的最大作業系統版本
MaxOsVersionWipe	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 含動作的最大作業系統版本清除資料
MinAppVersion	"0.0" = 無最低應用程式版本 其他任何專案 = 最低應用程式版本	■: 條件式發佈 ■: 具有動作區塊存取的最小應用程式版本
MinAppVersionWarning	"0.0" = 無最低應用程式版本。 其他任何專案 = 最低應用程式版本	■: 條件式發佈 ■: 具有動作警告的最小應用程式版本
MinAppVersionWipe	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作的最小應用程式版本清除資料
MinOsVersion	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作區塊存取的最小作業系統版本

名稱	說明	MICROSOFT 建議值
MinOsVersionWarning	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作警告的最小作業系統版本
MinOsVersionWipe	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 含動作的最小作業系統版本清除資料
MinSDKVersion	"0.0" = 無最低的 SDK 版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作區塊存取的最小 SDK 版本
MinSDKVersionWipe	"0.0" = 無最低的 SDK 版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作區塊存取的最小 SDK 版本
MinimumRequiredDeviceThreatProtectionLevel	0 = 未設定 1 = 安全 2 = 低 3 = 中速 4 = 高	■: 條件式發佈 ■: 允許的最大裝置威脅層級
MobileThreatDefenseRemediationAction	0 = 封鎖存取 1 = 擦除資料	■: 存取需求 ■: 允許的最大裝置威脅層級動作)
NonBioPassTimeOutRequired	0 = 非必要 1 = 需要	■: 存取需求 ■: 以 PIN 碼超時後覆寫觸控識別碼
NonBioPassTimeOut	x 分鐘	■: 存取需求 ■: 以 PIN 碼超時 > 超時, 覆寫觸控識別碼超時 (分鐘非使用中)
NotificationRestriction	0 = 允許 1 = 封鎖組織資料 2 = 封鎖	■: 資料保護 ■: Org data 通知
OpenDataFromManagedLocations	值, 代表應用程式可儲存資料的受管理儲存位置數目。 1 = OneDrive 2 = SharePoint 3 = OneDrive 和 SharePoint 4 = 相機 5 = OneDrive & 相機 6 = SharePoint & 相機 7 = 相機、OneDrive 和 SharePoint	■: 資料保護 ■: 允許使用者開啟選取服務中的資料
OpenDataIntoOrgDocumentsBlocked	0 = 允許 1 = 封鎖	■: 資料保護 ■: 開啟組織檔中的資料
OfflineWipeInterval	x 天	■: 此設定沒有系統管理控制。
PINCharacterType	0 = 密碼 1 = 數值	■: 存取需求 ■: Pin 類型
PINEnabled	0 = 非必要 1 = 需要	■: 存取需求 ■: 存取權的 PIN 碼
PINExpiryDays	x 個字元	■: 存取需求 ■: 在天數 > 天數後重設 PIN 碼的數目

名稱	說明	MICROSOFT 說明
PINMinLength	x 個字元	■: 存取需求 ■: 選取最小 PIN 碼長度
PINNumRetry	x 次嘗試	■: 條件式發佈 ■: PIN 碼嘗試次數上限
PrintingBlocked	0 = 允許 1 = 封鎖	■: 資料保護 ■: 列印組織資料
ProtectAllIncomingUnknownSourceData	不適用	■: Intune 服務未主動使用。
ProtectManagedOpenInData	0 = False 1 = True	■: 資料保護 ■: 若為 true, 將組織資料傳送至其他應用程式, 則會設定為使用開啟/共用篩選的原則管理應用程式。請注意, 當啟用具有作業系統共用的原則管理應用程式時, 也可以設定為 1。
ProtocolExclusions	應用程式 URL 通訊協定架構的清單, 可讓資料在對應的未受管理的應用程式資料中開啟	■: 資料保護 ■: 選取要免除的應用程式
RequireFileEncryption	不適用	■: Intune 服務未主動使用。
SimplePINAllowed	0 = 封鎖 1 = 允許	■: 存取需求 ■: 簡易 PIN
SpecificDialerProtocol	從受管理的應用程式通話所用之特定撥號器的 URL 通訊協定配置	■: 資料保護 ■: 撥號器應用程式 URL 配置
ThirdPartyKeyboardsBlocked	0 = 允許 1 = 封鎖	■: 資料保護 ■: 協力廠商鍵盤
TouchIDEnabled	0 = 封鎖 1 = 允許	■: 存取需求 ■: 觸控識別碼, 而不是使用 PIN 存取 (iOS 8 +/iPadOS)
UniversalLinkExclusions	通用連結清單, 可讓您在對應的非管理應用程式中開啟資料	■: 資料保護 ■: 選取要免除的通用連結
UnmanagedBrowserProtocol	用於查看受管理網頁連結之非管理瀏覽器的 URL 通訊協定配置	■: 資料保護 ■: 限制與其他應用程式的 web 內容傳輸

Android 應用程式防護原則設定

名稱	說明	MICROSOFT 說明
AccessRecheckOfflineTimeout	x 分鐘	■: 條件式發佈 ■: 具有動作區塊存取的離線寬限期 (分鐘)

名稱	說明	MICROSOFT 說明
AccessRecheckOnlineTimeout	x 分鐘	■: 存取需求 ■: 在 (分鐘) 的非活動狀態之後重新檢查存取需求)
AllowedAndroidManufacturersElseBlock	若未設定, 則為空, 否則為允許的製造商清單	■: 條件式發佈 ■: 具有動作的裝置製造商指定的 (區塊未指定)
AllowedAndroidManufacturersElseWipe	若未設定, 則為空, 否則為允許的製造商清單	■: 條件式發佈 ■: 具有動作的裝置生產商允許指定 (清除非指定的)
AllowedAndroidModelsElseBlock	若未設定, 則為空, 否則為允許的模型清單	此設定沒有管理控制權。
AllowedAndroidModelsElseWipe	若未設定, 則為空, 否則為允許的模型清單	此設定沒有管理控制權。
AndroidSafetyNetDeviceAttestationEnforcement	NOT_REQUIRED = 未設定 BASIC_INTEGRITY = 基本完整性 BASIC_INTEGRITY_AND_DEVICE_CERTIFICATION = 基本的完整性及驗證裝置	■: 條件式發佈 ■: SafetyNet 裝置認證
AndroidSafetyNetDeviceAttestationFailedAction	BLOCK = 封鎖存取 警告 = 警告 WIPE_DATA = 清除資料	■: 條件式發佈 ■: SafetyNet 裝置認證
AndroidSafetyNetVerifyAppsEnforcementType	NOT_REQUIRED = 未設定 REQUIRE_ENABLED = 設定	■: 條件式發佈 ■: 需要在應用程式上進行威脅掃描
AndroidSafetyNetVerifyAppsFailedAction	BLOCK = 封鎖存取 警告 = 警告	■: 條件式發佈 ■: 需要在應用程式上進行威脅掃描
AppActionIfUnableToAuthenticateUser	NONE = 未設定 BLOCK = 封鎖存取 WIPE_DATA = 清除應用程式	■: 條件式發佈 ■: 停用帳戶
AppPinDisabled	true = 需要 false = 非必要	■: 存取需求 ■: 裝置 pin 碼設定時的應用程式 PIN 碼
ApprovedKeyboards	IDs 必要的核准鍵盤捆綁清單	■: 資料保護 ■: 選取要核准的鍵盤
AppSharingFromLevel	封鎖 = 無 MANAGED = 原則管理的應用程式 無限制 = 所有應用程式	■: 資料保護 ■: 從其他應用程式接收資料
AppSharingToLevel	封鎖 = 無 MANAGED = 原則管理的應用程式 無限制 = 所有應用程式	■: 資料保護 ■: 將組織資料傳送至其他應用程式
AuthenticationEnabled	false = 非必要 true = 需要	■: 存取需求 ■: 存取的工作單位或學校帳號憑證

名稱	說明	MICROSOFT 說明
BiometricIdEnabled	0 = 封鎖 1 = 允許	■:存取需求 ■:生物識別的生物特徵, 而不是 PIN 存取權
BlockAfterCompanyPortalUpdateDeferralInDays	x 天	■:條件式發佈 ■:最大公司入口網站版本壽命 (天數)
BlockClockStatusWithGracePeriod	不適用	■: Intune 服務未主動使用。
BlockScreenCapture	false = 允許 true = 封鎖	■:資料保護 ■:螢幕截圖和 Google Assistant
ClipboardCharacterExceptionLength	x 個字元	■:資料保護 ■:剪下及複製任何應用程式的字元限制
ClipboardSharingLevel	封鎖 = 封鎖 MANAGED = 原則管理的應用程式 MANAGED_PASTE_IN = 具有貼上的原則管理應用程式 非管理 = 任何應用程式	■:資料保護 ■:限制其他應用程式之間的剪下、複製和貼上
ConditionalEncryptionEnabled	false = 需要 true = 非必要	■:資料保護 ■:加密已註冊裝置上的組織資料
ConnectToVPNOnLaunch	不適用	■: Intune 服務未主動使用。
ContactSyncDisabled	false = 允許 true = 封鎖	■:資料保護 ■:使用原生連絡人應用程式的 Sync 應用程式
DataBackupDisabled	false = 允許 true = 封鎖	■:資料保護 ■:防止備份
DeviceComplianceEnabled	false = False true = True	■:條件式發佈 ■:已越獄/有根的裝置
DeviceComplianceFailureAction	BLOCK = 封鎖存取 WIPE_DATA = 清除資料	■:條件式發佈 ■:已越獄/有根的裝置
DialerRestrictionLevel	0 = 無, 請勿在應用程式之間傳輸此資料 1 = 特定撥號器應用程式 2 = 任何原則管理的撥號器應用程式 3 = 任何撥號器應用程式	■:資料保護 ■:將電信資料傳輸至
DictationBlocked	false = 允許 true = 封鎖	此設定沒有管理控制權。
FileEncryptionKeyLength	128 256	此設定沒有管理控制權。
FileSharingSaveAsDisabled	false = 允許 true = 封鎖	■:資料保護 ■:儲存組織資料的副本

名稱	說明	MICROSOFT 說明
IntuneMAMPolicyVersion	版本號碼	不適用
isManaged	真假	不適用
KeyboardsRestricted	true = 必要 false = 非必要	■: 資料保護 ■: 核准的鍵盤
ManagedBrowserRequired	true = Microsoft Edge 或未受管理的瀏覽器 false = 任何應用程式	■: 資料保護 ■: 將 web 內容傳輸限制為其他應用程式應用程式。
ManagedLocations	一個值, 代表應用程式可以儲存資料的受管理儲存位置數目 (以分號分隔)。 ONEDRIVE_FOR_BUSINESS SHAREPOINT 當地	■: 資料保護 ■: 允許使用者將副本儲存到選取的服務
MaxPinRetryExceededAction	RESET_PIN = 重設 PIN 碼 WIPE_DATA = 清除資料	■: 條件式發佈 ■: PIN 碼嘗試次數上限
MaxOsVersion	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 具有動作區塊存取的最大作業系統版本
MaxOsVersionWarning	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 具有動作警告的最大作業系統版本
MaxOsVersionWipe	"0.0" = 無最大 OS 版本 其他任何專案 = 作業系統最高版本	■: 條件式發佈 ■: 含動作的最大作業系統版本清除資料
MinAppVersion	"0.0" = 無最低應用程式版本 其他任何專案 = 最低應用程式版本	■: 條件式發佈 ■: 具有動作區塊存取的最小應用程式版本
MinAppVersionWarning	"0.0" = 無最低應用程式版本。 其他任何專案 = 最低應用程式版本	■: 條件式發佈 ■: 具有動作警告的最小應用程式版本
MinAppVersionWipe	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作的最小應用程式版本清除資料
MinOsVersion	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作區塊存取的最小作業系統版本
MinOsVersionWarning	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 具有動作警告的最小作業系統版本
MinOsVersionWipe	"0.0" = 無最低作業系統版本 其他任何專案 = 最低作業系統版本	■: 條件式發佈 ■: 含動作的最小作業系統版本清除資料
MinPatchVersion	"0000-00-00" = 無最低的修補程式版本 其他任何專案 = 最低修補程式版本	■: 條件式發佈 ■: 具有 action 封鎖存取的修補程式版本最小

名稱	類型	MICROSOFT 說明
PINCharacterType	密碼 = 密碼 數值 = 數值	■: 存取需求 ■: Pin 類型
PINEnabled	false = 非必要 true = 需要	■: 存取需求 ■: 存取權的 PIN 碼
PINExpiryDays	x 個字元	■: 存取需求 ■: 在天數 > 天數後重設 PIN 碼的數目
PINMinLength	x 個字元	■: 存取需求 ■: 選取最小 PIN 碼長度
PINNumRetry	x 次嘗試	■: 條件式發佈 ■: PIN 碼嘗試次數上限
PackageExclusions	若未設定任何束 IDs, 則為空, 否則會以分號分隔 IDs	■: 資料保護 ■: 選取要免除的應用程式
PinHistoryLength	要維護的 x PIN 碼值	■: 存取需求 ■: 選取要維護的先前 PIN 碼值數目
PolicyCount	number	不適用
PrintingBlocked	false = 允許 true = 封鎖	■: 資料保護 ■: 列印組織資料
RequireDeviceLock	true = 必要 false = 非必要	■: 條件式發佈 ■: 需要鎖定裝置
RequireDeviceLockEnforcementType	BLOCK = 封鎖存取 WIPE_DATA = 需要擦除	■: 條件式發佈 ■: 需要鎖定裝置
RequireFileEncryption	false = 非必要 true = 需要	■: 資料保護 ■: 加密組織資料
SimplePINAllowed	false = 封鎖 true = 允許	■: 存取需求 ■: 簡易 PIN
SpecificDialerDisplayName	撥號器應用程式名稱	■: 資料保護 ■: 撥號器應用程式名稱
SpecificDialerPackageID	撥號器應用程式束識別碼	■: 資料保護 ■: 撥號器應用程式套件識別碼
TouchIDEnabled	false = 封鎖 true = 允許	■: 存取需求 ■: 指紋, 而不是使用 PIN 存取 (Android 9.0 +)
UnmanagedBrowserDisplayName	未受管理的網頁瀏覽器顯示名稱	■: 資料保護 ■: 非受管理的瀏覽器名稱
UnmanagedBrowserPackageID	非管理網頁瀏覽器套件識別碼	■: 資料保護 ■: 非管理的瀏覽器識別碼

名稱	說明	MICROSOFT 建議值
UserStatusPollInterval	不適用	■: Intune 服務未主動使用。
UserStatusTimeoutInSeconds	不適用	■: Intune 服務未主動使用。

後續步驟

- 若要深入瞭解應用程式保護原則，請參閱 [什麼是應用程式保護原則？](#)
- Intune 提供許多工具，協助您疑難排解環境中的問題。如需詳細資訊，請參閱 [使用疑難排解入口網站協助使用者](#)。

Microsoft Intune App SDK 概觀

2022/9/27 •

iOS 和 Android 皆可使用的 Intune 應用程式 SDK，可讓您的應用程式支援 Intune [應用程式保護原則](#)。當您的應用程式已對其套用應用程式防護原則時，它可以由 Intune 管理，且 Intune 會識別為受管理的應用程式。SDK 致力於將應用程式開發人員所需的程式碼變更量降至最低。您會發現，您可以在不變更應用程式行為的情況下，啟用大部分的 SDK 功能。為了增強使用者和 IT 管理員的體驗，您可以利用 SDK 的 APIs 自訂應用程式行為，以支援需要您的應用程式參與的功能。

當您啟用您的應用程式以支援 Intune 應用程式保護原則之後，IT 系統管理員可以部署這些原則，以保護其在應用程式內的公司資料。

應用程式保護功能

以下是可與 SDK 一起啟用之 Intune 應用程式保護功能的範例。

控制使用者移動公司檔案的能力

IT 管理員可以控制應用程式中的工作或學校資料可以移動的位置。例如，他們可以部署停用應用程式將公司資料備份至雲端的原則。

設定剪貼簿限制

IT 管理員可以在 Intune 管理的應用程式中設定剪貼簿行為。例如，他們可以部署原則，以防止使用者從應用程式中剪切或複製資料，並貼到未受管理的個人應用程式。

在儲存的資料上強制加密

IT 系統管理員可以強制執行原則，以確保應用程式儲存至裝置的資料已加密。

遠端擦除公司資料

IT 系統管理員可以從 Intune 管理的應用程式中遠端擦除公司資料。這項功能是以身分識別為基礎，且只會刪除與使用者之公司身分識別相關聯的檔案。若要這麼做，此功能需要應用程式參與。應用程式可以根據使用者設定，指定要進行擦除的身分識別。在應用程式中沒有這些指定的使用者設定時，預設行為是清除應用程式目錄，並通知使用者已移除存取權。

強制使用 managed browser

IT 管理員可以強制使用 [Intune Managed Browser 應用程式](#) 開啟應用程式中的網頁連結。這項功能可確保出現在公司環境中的連結會保留在 Intune 管理的應用程式網域內。

強制執行 PIN 原則

IT 系統管理員可要求使用者在存取應用程式中的公司資料之前輸入 PIN 碼。這可確保使用此應用程式的人員與最初登入公司或學校帳戶的人員相同。當使用者設定其 PIN 碼時，Intune 應用程式 SDK 會使用 Azure Active Directory，對照已註冊的 Intune 帳戶驗證使用者的認證。

要求使用者使用工作或學校帳戶登入應用程式存取

IT 系統管理員可要求使用者利用其工作或學校帳戶登入，以存取應用程式。Intune 應用程式 SDK 使用 Azure Active Directory 來提供單一登入體驗，以供後續登入在重新輸入認證時使用。我們也支援與 Azure Active Directory 同盟的身分識別管理解決方案的驗證。

檢查裝置健康情況和合規性

IT 管理員可以檢查裝置的健康情況，以及其與 Intune 原則的相容性，使用者才能存取應用程式。在 iOS/iPadOS 上，此原則會檢查裝置是否已越獄。在 Android 上，此原則會檢查裝置是否為根。

支援多重身分識別

多身分識別支援是 SDK 的一項功能，可讓單一應用程式中原則管理的 (公司) 和非管理 (個人) 帳戶共存。

例如，許多使用者在 iOS 和 Android 的 Office 行動應用程式中設定公司和個人電子郵件帳戶。當使用者以公司帳戶存取資料時，IT 系統管理員必須確信將套用應用程式保護原則。不過，當使用者存取個人電子郵件帳戶時，該資料應該會位於 IT 管理員的控制之外。在 Intune 應用程式 SDK 中，只會將應用程式保護原則導向至應用程式中的公司身分識別。

「多身分識別」功能可協助解決組織面臨的資料保護問題，使其可支援個人和工作帳戶的儲存應用程式。

無裝置註冊的應用程式保護

IMPORTANT

Intune 應用程式防護工具、適用於 Android 的 intune 應用程式 SDK、適用於 iOS 的 intune 應用程式 sdk，以及 Intune 應用程式 SDK Xamarin 系結，均可搭配使用 intune 應用程式的裝置註冊。

許多具有個人裝置的使用者都想要存取公司資料，而不是使用行動裝置管理 (MDM) 提供者來註冊其個人裝置。由於 MDM 註冊需要裝置的全域控制，使用者常常會 hesitant 將其個人裝置的控制權交給公司。

無裝置註冊的應用程式保護可讓 Microsoft Intune 服務直接將應用程式保護原則部署至應用程式，而不需依賴裝置管理通道來部署原則。

隨 Citrix mVPN 的隨選應用程式 VPN 連線

您可以使用 Citrix XenMobile MDX 和 Microsoft Intune 的組合，管理裝置和應用程式。此結合意味著您可以使用 Citrix 的 mVPN 技術，管理具有 Intune 應用程式保護原則的應用程式。與 Citrix 的整合可用於 iOS 和 Android 的 intune 應用程式 SDK，以及使用 Citrix 旗標 iOS (的 intune App Wrapping Tool)。

若要深入瞭解 Citrix MDX，請參閱 [關於 MDX 工具](#)、[citrix mdx 應用程式封裝的 iOS](#)，以及 [適用於 Android 的 citrix mdx 應用程式封裝](#)。

後續步驟

- [開始使用 Microsoft Intune 應用程式 SDK](#)。

使用 Microsoft Intune App SDK 開始

2022/9/27 •

本指南將協助您快速啟用行動應用程式，以透過Microsoft Intune支援應用程式保護原則。如 Intune [App SDK 概觀](#)中所述，您可能會發現先瞭解 Intune App SDK 的優點很有用。

Intune App SDK 支援跨 iOS 和 Android 的類似案例，旨在為 IT 系統管理員建立跨平臺的一致體驗。但是，由於平臺差異和限制，支援特定功能的差異很小。

向 Microsoft 註冊您的市集應用程式

如果您的應用程式是組織內部，且無法公開使用：

您 **不需要** 註冊您的應用程式。針對內部 [企業營運 \(LOB\)](#) 公司或公司所撰寫的應用程式，IT 系統管理員會在內部部署應用程式。Intune會偵測到應用程式已使用 SDK 建置，並可讓 IT 系統管理員將應用程式保護原則套用至該應用程式。您可以跳到 [啟用您的 iOS 或 Android 應用程式以取得應用程式保護原則](#)一節。

如果您的應用程式將會發行至公用應用程式市集，例如 [Apple App Store](#) 或 [Google Play](#)：

您 **必須** 先向Microsoft Intune註冊您的應用程式，並同意註冊條款。然後，IT 系統管理員可以將應用程式保護原則套用至受控應用程式，這會列為 [合作夥伴生產力應用程式](#)。

在註冊完成並由Microsoft Intune小組確認之前，Intune系統管理員將無法選擇將應用程式保護原則套用至應用程式的深層連結。Microsoft 也會將您的應用程式新增至其[\[Microsoft Intune 合作夥伴\]](#) 頁面。在該處，將會顯示應用程式的圖示，以顯示它支援Intune應用程式保護原則。

註冊程式

若要開始註冊程式，如果您尚未與 Microsoft 連絡人合作，請填寫[Microsoft Intune應用程式合作夥伴問卷](#)。

我們將使用問卷回應中列出的電子郵件地址來聯繫並繼續註冊程式。此外，如果我們有任何疑慮，我們會使用您的註冊電子郵件地址與您連絡。

NOTE

問卷中收集的所有資訊，以及透過與Microsoft Intune小組的電子郵件通訊，都會接受[Microsoft 隱私權聲明](#)。

註冊程式中的預期事項：

1. 提交問卷之後，我們會透過您的註冊電子郵件地址與您連絡，以確認成功收據或要求其他資訊以完成註冊。
2. 從您收到所有必要資訊之後，我們會將要簽署的Microsoft Intune應用程式合作夥伴合約傳送給您。本合約說明貴公司成為Microsoft Intune應用程式合作夥伴之前必須接受的條款。
3. 當您的應用程式成功向Microsoft Intune服務註冊，以及您的應用程式在Microsoft Intune合作夥伴網站上顯示時，您會收到通知。
4. 最後，您的應用程式深層連結會新增至下一個每月Intune服務更新。例如，如果註冊資訊在 7 月完成，則 8 月中將支援深層連結。

深層連結是公用應用程式市集中應用程式清單的連結。如果您應用程式的深層連結在未來有所變更，您必須重新註冊您的應用程式。

下載 SDK 檔案

原生 iOS 和 Android 的 Intune 應用程式 SDK 裝載于 Microsoft GitHub 帳戶上。這些公用存放庫分別具有原生 iOS 和 Android 的 SDK 檔案：

- [適用於 iOS 的 Intune App SDK](#)
- [適用於 Android 的 Intune App SDK](#)

如果您的應用程式是 Xamarin 應用程式，請使用此 SDK 變體：

- [Intune App SDK Xamarin Bindings](#)

建議您註冊 GitHub 帳戶，以使用來分岔和從我們的存放庫提取。GitHub 可讓開發人員與我們的產品小組通訊、開啟問題並接收快速回應、檢視版本資訊，以及提供意見反應給 Microsoft。如需有關 Intune App SDK GitHub 的問題，請連絡 msintuneappsdk@microsoft.com。

針對應用程式保護原則啟用您的 iOS 或 Android 應用程式

您將需要下列其中一個開發人員指南，以協助您將 Intune App SDK 整合到您的應用程式中：

- [Intune 適用於 iOS 的 App SDK 開發人員指南](#)：本檔將逐步引導您使用 Intune App SDK 啟用原生 iOS 應用程式。
- [Intune App SDK for Android 開發人員指南](#)：本檔將逐步引導您使用 Intune App SDK 啟用原生 Android 應用程式。
- [Intune 應用程式 SDK Xamarin 系結指南](#)：本檔將協助您使用 Xamarin 建置 iOS 和 Android 應用程式，以 Intune 應用程式保護原則。

IMPORTANT

Intune 定期發行 Intune App SDK 的更新。定期檢查 [Intune App SDK](#) 存放庫是否有更新，並併入您的軟體發展發行週期，以確保您的應用程式支援最新的應用程式保護原則設定。

針對以應用程式為基礎的條件式存取啟用您的 iOS 或 Android 應用程式

除了啟用應用程式的應用程式保護原則之外，您的應用程式還需要下列專案，才能正確地與 Azure Active Directory (AAD) 應用程式型條件式存取搭配運作：

- 應用程式是使用 [Microsoft 驗證程式庫](#) 所建置，並已啟用 AAD 訊息代理程式驗證。
- [您應用程式 AAD 用戶端標識符](#) 在 iOS 和 Android 平臺上必須是唯一的。

設定應用程式的遙測

Microsoft Intune 收集應用程式使用量統計資料的資料。

- **Intune 適用於 iOS 的 App SDK**：SDK 預設會記錄使用事件的 SDK 遙測資料。此資料會傳送至 Microsoft Intune。
 - 如果您選擇不從應用程式傳送 SDK 遙測資料至 Microsoft Intune，您必須在 IntuneMAMSettings 字典中將屬性 `MAMTelemetryDisabled` 設定為 "YES" 來停用遙測傳輸。
- **Intune App SDK for Android**：Intune App SDK for Android 不會控制來自您應用程式的資料收集。公司入口網站應用程式預設會記錄遙測資料。此資料會傳送至 Microsoft Intune。根據 Microsoft 原則，我們不會收集 PII (任何個人識別資訊)。
 - 如果終端使用者選擇不傳送此資料，則必須在公司入口網站應用程式的設定下關閉遙測。若要深入瞭

解，請 [參閱關閉 Microsoft 使用量資料收集](#)。

企業營運應用程式版本號碼

Intune中的企業營運應用程式現在會顯示 iOS 和 Android 應用程式的版本號碼。此數位會顯示在應用程式清單和應用程式概觀刀鋒視窗中[Microsoft 端點管理員系統管理中心](#)。終端使用者可以在公司入口網站應用程式和入口網站中看到應用程式號碼。

完整版本號碼

完整版本號碼會識別應用程式的特定版本。此數位會顯示為 *版本 (組建)*。例如, 2.2 (2.2.17560800)。

完整版本號碼有兩個元件：

- **版本**

版本號碼是應用程式的人類可讀取版本號碼。使用者會使用此功能來識別不同版本的應用程式。

- **組建編號**

組建編號是內部編號，可用於應用程式偵測和以程式設計方式管理應用程式。組建編號是指參考程式碼中變更的應用程式反復專案。

Android 和 iOS 中的版本和組建編號

Android 和 iOS 都會在應用程式參考中使用版本和組建編號。不過，這兩個作業系統都有作業系統特定的意義。下表說明這些詞彙的相關性。

當您開發企業營運應用程式以用於Intune時，請記得同時使用版本和組建編號。Intune應用程式管理功能依賴適用於 Android) 的 iOS) 和 PackageVersionCode (有意義的 CFBundleVersion (。這些數位會包含在應用程式資訊清單中。

INTUNE	IOS	ANDROID	II
版本號碼	CFBundleShortVersionString	PackageVersionName	此數位表示特定版本的使用者應用程式。
組建編號	CFBundleVersion	PackageVersionCode	此數位可用來指出應用程式程式碼中的反復專案。

iOS

- **CFBundleShortVersionString**

指定套件組合的發行版本號碼。此號碼會識別應用程式的發行版本。使用者會使用此數位來參考應用程式。

- **CFBundleVersion**

套件組合的組建版本，可識別套件組合的反復專案。此數位可以識別發行或未發行的套件組合。此數目用於應用程式偵測。

Android

- **PackageVersionName**

向使用者顯示的版本號碼。這個屬性可以設定為原始字串或字串資源的參考。字串除了要向使用者顯示之外，沒有其他用途。

- **PackageVersionCode**

內部版本號碼。此數位僅用來判斷某個版本是否比另一個版本更新，且數位越高，表示較新的版本。這不是版本

整合後的後續步驟

測試您的應用程式

完成整合 iOS 或 Android 應用程式與 Intune App SDK 的必要步驟之後，您必須確定所有應用程式保護原則都已

針對使用者和 IT 系統管理員啟用並正常運作。若要測試整合式應用程式，您需要下列專案：

- **Microsoft Intune測試帳戶**：若要針對Intune應用程式保護功能測試受Intune管理的應用程式，您需要Microsoft Intune帳戶。
 - 如果您是針對Intune應用程式保護原則啟用 iOS 或 Android 市集應用程式的 ISV，您會在完成註冊後收到促銷代碼Microsoft Intune，如註冊步驟中所述。促銷程式碼可讓您註冊Microsoft Intune試用版，以獲得一年的延長使用期。
 - 如果您正在開發不會隨附至市集的企業營運應用程式，您應該能夠透過組織存取Microsoft Intune。您也可以Microsoft Intune 中註冊一個月的免費試用版。
 - 如果您要使用使用者帳戶在行動裝置上測試應用程式，請確定您在使用系統管理員帳戶登入之後，已在Microsoft 365 系統管理中心網站中為該帳戶提供Intune授權，請參閱[指派Microsoft Intune授權](#)。
- **Intune應用程式保護原則**：若要針對所有Intune應用程式保護原則來測試您的應用程式，您應該知道每個原則設定的預期行為。請參閱 [iOS 應用程式保護原則](#) 和 [Android 應用程式保護原則](#) 的描述。如果您的應用程式已整合Intune SDK，但未列在可設定目標的應用程式清單中，您可以在選取 [自訂應用程式] 時，在文字方塊中指定應用程式的套件組合識別碼 (iOS) 或套件名稱 (Android)。
- **疑難排解**：如果您在手動測試應用程式的安裝使用者體驗時遇到任何問題，請參閱 [針對應用程式安裝問題進行疑難排解](#)。

將應用程式存取權授與Intune應用程式保護服務 (選擇性)

如果您的應用程式使用自己的自訂Azure Active Directory (AAD) 設定進行驗證，則應該針對公用市集應用程式和內部 LOB 應用程式採取下列步驟。如果您的 **應用程式使用 Intune SDK 預設用戶端標識符**，則不需要採取這些步驟。

一旦您已在 Azure 租使用者中註冊應用程式，且應用程式會顯示在 [所有應用程式] 底下，您必須將應用程式存取權授與Intune應用程式保護服務，(先前稱為 MAM 服務)。在[Microsoft 端點管理員 系統管理中心](#)：

1. 移至 [Azure Active Directory] 刀鋒視窗。
2. 在 [應用程式註冊] 底下，移至為應用程式設定的清單。
3. 按一下 [+ 新增許可權]。
4. 按一下 **我的組織所使用的 API**。
5. 在搜尋方塊中，輸入 Microsoft Mobile Application Management。
6. 在 [委派的許可權] 下，選取 [DeviceManagementManagedApps.ReadWrite：讀取和寫入使用者的應用程式管理資料] 核取方塊。
7. 按一下 [新增許可權]。

NOTE

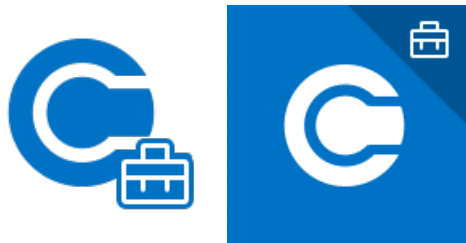
如果您的應用程式因為存取此資源時發生錯誤而限制您登入：HTTPS://intunemam.microsoftonline.com，您必須使用應用程式的用戶端識別碼傳送附注給 msintuneappsdk@microsoft.com。這是現今的手動核准程式。

為您的應用程式 (選用) 徽章

驗證Intune應用程式保護原則可在您的應用程式中運作之後，您可以使用Intune應用程式保護標誌來為應用程式圖示加上徽章。

此徽章向 IT 系統管理員、使用者和潛在Intune客戶指出您的應用程式可與Intune應用程式保護原則搭配使用。它鼓勵Intune客戶使用和採用您的應用程式。

徽章是公事包圖示，如下列範例所示：



您需要什麼才能為您的應用程式徽章：

- 可讀取 .eps 檔案的 影像操作應用程式, 或可讀取 .ai 檔案的 Adobe 應用程式。
- 您可以在Microsoft Intune GitHub上找到[Intune應用程式徽章資產和指導方針](#)。

準備應用程式保護原則的企業營運應用程式

2022/9/27 •

您可以使用 Intune App Wrapping Tool 或 Intune 應用程式 SDK，讓應用程式使用應用程式保護原則。使用此資訊來瞭解這兩種方法及使用時機。

Intune App Wrapping Tool

App Wrapping Tool 主要用於內部公司營運 (LOB) 應用程式。此工具是一種命令列應用程式，它會在應用程式上建立包裝，然後允許 Intune 應用程式保護原則管理應用程式。當保護獨立軟體廠商所提供的應用程式 (ISV)，請務必明確 ISV 是否仍支援包裝應用程式。

您不需要使用此工具的原始程式碼，但需要簽署認證。如需簽署認證的詳細資訊，請參閱 [Intune 博客](#)。如需 App Wrapping Tool 檔，請參閱 [Android App Wrapping Tool](#) 和 [iOS App Wrapping Tool](#)。

App Wrapping Tool 不支援 Apple App store 或 Google Play Store 中或提供的應用程式。它也不支援需要開發人員整合的某些功能 (請參閱下列功能比較表)。

如需有關未在 Intune 中註冊之裝置上應用程式保護原則 App Wrapping Tool 的詳細資訊，請參閱 [保護業務營運應用程式](#)，以及在未登記 Microsoft Intune 裝置上的資料。

IMPORTANT

Intune 定期發佈 Intune App Wrapping Tool 的更新。定期檢查 [Intune App Wrapping Tool](#) 存放庫以取得更新，並併入您的軟體發展發行週期，以確保您的應用程式支援最新的應用程式保護原則設定。

使用 App Wrapping Tool 的原因

- 您的應用程式沒有內建的資料保護功能
- 您的應用程式已在內部部署，且應用程式無法在 Apple 應用程式存放區或 Google Play 存放區中使用
- 您無法存取應用程式的原始程式碼
- 您沒有開發應用程式
- 您的應用程式的使用者驗證經驗極少

支援的應用程式開發平臺

APP WRAPPING TOOL	XAMARIN	
iOS	是	是
Android	No-使用 Intune 應用程式 SDK Xamarin 系結。	是

Intune 應用程式 SDK

應用程式 SDK 主要專為在 Apple 應用程式存放區或 Google Play 商店中有應用程式的客戶，而且想要能夠使用 Intune 管理應用程式。不過，任何應用程式都可以利用整合 SDK，甚至是商務營運營運應用程式。

若要深入瞭解 SDK，請參閱 [一覽](#)。若要開始使用 SDK，請參閱 [Microsoft Intune 應用程式 SDK 快速入門](#)。

使用 SDK 的原因

- 您的應用程式沒有內建的資料保護功能

- 您的應用程式部署在公用應用程式存放區(如 Google Play 或 Apple 的應用程式存放區)上
- 您是應用程式開發人員，具有使用 SDK 的技術背景
- 您的應用程式有其他 SDK 整合
- 您的應用程式經常更新

支援的應用程式開發平臺

INTUNE 開發 SDK	XAMARIN	開發
iOS	是—使用 Intune 應用程式 SDK Xamarin 系結。	否
Android	是, 使用 Intune 應用程式 SDK Xamarin 系結。	否

不使用以上所列的應用程式開發平臺嗎？

Intune SDK 開發小組會積極測試及維護使用原生 Android (iOS (Obj-C、Swift) 、Xamarin 及 Xamarin.Forms 平臺)所建立的應用程式的支援。不會提供其他平臺的指導方針，但是可以使用原生 SDK 來建立您自己的外掛程式。

功能比較

此表格列出當應用程式使用應用程式 SDK 或 App Wrapping Tool 時所啟用的設定。有些功能需要應用程式開發人員將基本整合以外的某些邏輯套用至 Intune SDK, 如此一來，如果應用程式使用 App Wrapping Tool, 就不會啟用。

功能	開發 SDK	APP WRAPPING TOOL
將網站內容限制在公司受管理的瀏覽器中顯示	X	X
避免 Android、iTunes 或 iCloud 備份	X	X
允許應用程式將資料傳送到其他應用程式	X	X
[允許應用程式接收其他應用程式的資料]	X	X
限制利用其他應用程式剪下、複製及貼上	X	X
指定受管理的應用程式可能會剪下或複製的字元數	X	X
需要簡單 PIN 碼才能存取	X	X
指定重設 PIN 之前的嘗試次數	X	X
允許指紋而非 PIN	X	X
只允許面部認可，而不是 PIN (iOS)	X	X

II	IIII SDK	APP WRAPPING TOOL
需要公司認證才能存取	X	X
設定 PIN 碼到期	X	X
封鎖受管理的應用程式在已進行 JB 或 Root 破解的裝置上執行	X	X
加密應用程式資料	X	X
在指定的分鐘數之後重新檢查存取需求	X	X
指定離線寬限時間	X	X
僅限 Android (封鎖螢幕抓)	X	X
不支援 device 註冊的 MAM	X	X
完全清除應用程式資料	X	X
選擇性擦除多身分識別案例中的工作和學校資料 ■: 若為 iOS/iPadOS, 當管理設定檔已移除時, 也會移除該應用程式。	X	
防止「另存新檔」	X	
目標應用程式設定 (或透過「MAM 通道」的應用程式佈建)	X	X
支援多身分識別	X	
可自訂樣式	X	
隨 Citrix mVPN 的隨選應用程式 VPN 連線	X	X
停用連絡人同步處理	X	X
停用列印	X	X
需要最小應用程式版本	X	X
需要最低作業系統	X	X
只需要最小 Android 安全性修補程式版本 (Android)	X	X
IOS (只需要最小的 Intune SDK iOS)	X	X
SafetyNet 裝置認證 (僅限 Android)	X	X

II	IIII SDK	APP WRAPPING TOOL
在應用程式上進行威脅掃描 (僅限 Android)	X	X
需要最大行動威脅防護廠商裝置風險層級	X	
設定組織帳戶的代理程式更新內容	X	X
需要使用核准的鍵盤 (僅限 Android)	X	X
需要應用程式保護原則 (條件式存取)	X	

後續步驟

若要深入瞭解應用程式保護原則及 Intune，請參閱下列主題：

- [Android 應用程式換行工具](#)
- [iOS 應用程式換行工具](#)
- [使用 SDK 啟用行動應用程式管理應用程式](#)

使用 Intune 應用程式包裝工具將 iOS 應用程式準備好使用應用程式防護原則

2022/9/27 •

使用適用於 iOS 的 Microsoft Intune App Wrapping Tool，在不變更應用程式本身的程式碼的情況下，啟用內部 iOS 應用程式的 Intune 應用程式保護原則。

此工具是 macOS 命令列應用程式，可在應用程式周圍建立包裝函式。處理應用程式之後，您可以藉由將 [應用程式保護](#) 原則部署至應用程式來變更應用程式的功能。

若要下載此工具，請參閱 [GitHub 上的 iOS Microsoft Intune App Wrapping Tool](#)。

NOTE

如果您在應用程式中使用 Intune App Wrapping Tool 時發生問題，請在 GitHub 上提交 [協助要求](#)。

App Wrapping Tool 的一般必要條件

執行 App Wrapping Tool 之前，您必須先滿足一些一般必要條件：

- 從 GitHub 下載 [適用於 iOS 的 Microsoft Intune App Wrapping Tool](#)。
- 已安裝 Xcode 工具組 14.0 版或更新版本的 macOS 電腦。
- 輸入 iOS 應用程式必須由您的公司或獨立軟體廠商開發及簽署，(ISV)。
 - 輸入應用程式檔案的副檔名必須是 .ipa 或 .app。
 - 輸入應用程式必須針對 iOS 14.0 或更新版本進行編譯。
 - 輸入應用程式無法加密。
 - 輸入應用程式不能有擴充的檔案屬性。
 - 輸入應用程式必須先設定權利，才能由 Intune App Wrapping Tool 處理。[權利會](#) 為應用程式提供比一般授與更多的許可權和功能。如需指示，請參閱 [設定應用程式權利](#)。

App Wrapping Tool 的 Apple 開發人員必要條件

若要以獨佔方式將包裝的應用程式散發給組織的使用者，您需要一個具有 [Apple Developer Enterprise Program](#) 的帳戶，以及連結至 Apple Developer 帳戶的數個應用程式簽署實體。

若要深入瞭解如何在內部將 iOS 應用程式散發給組織的使用者，請閱讀 [散發 Apple Developer Enterprise Program Apps](#) 的官方指南。

您將需要下列專案來散發由 Intune 包裝的應用程式：

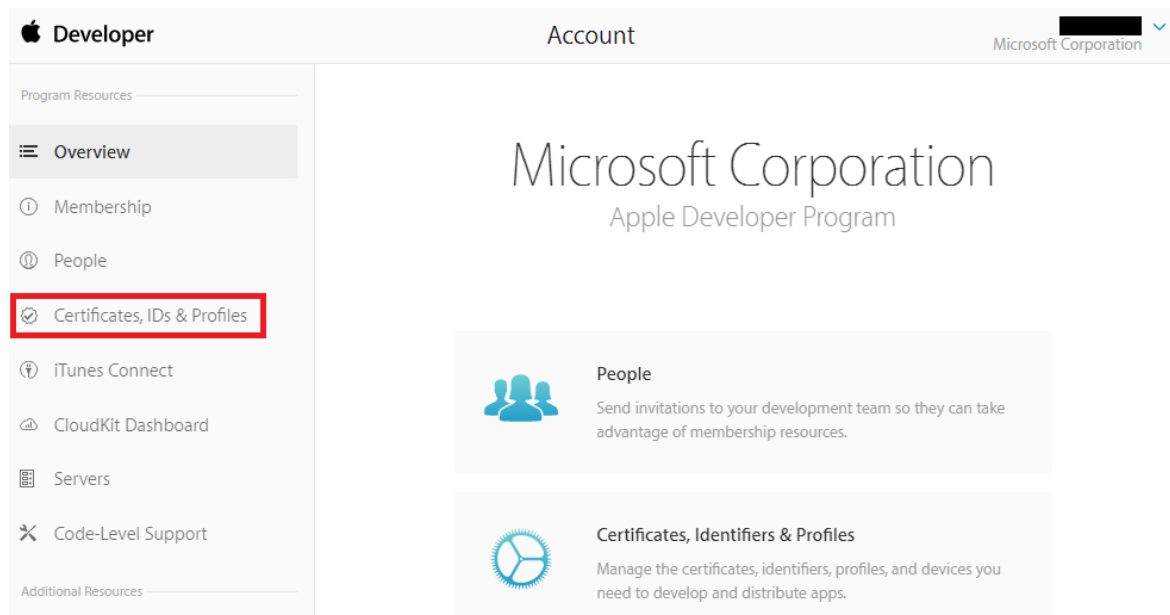
- Apple Developer Enterprise Program 的開發人員帳戶。
- 具有有效小組識別碼的內部和隨機操作散發簽署憑證。
 - 您需要簽署憑證的 SHA1 雜湊作為 Intune App Wrapping Tool 的參數。
- 內部散發布建設定檔。

建立 Apple Developer Enterprise 帳戶的步驟

1. 移至 [Apple Developer Enterprise Program 網站](#)。
2. 在頁面右上方, 按一下 [註冊]。
3. 閱讀您需要註冊專案的檢查清單。按一下頁面底部的 [開始註冊]。
4. 使用 組織的 Apple ID 登入。如果您沒有 Apple ID, 請按一下 [建立 Apple ID]。
5. 選取您的 實體類型, 然後按一下 [繼續]。
6. 在表單中填入您組織的資訊。按一下 [繼續]。此時, Apple 會連絡您, 確認您已獲授權註冊您的組織。
7. 驗證之後, 按一下 [同意授權]。
8. 同意授權之後, 請 購買並啟用方案來 完成。
9. 如果您是小組代理程式 (代表貴組織加入 Apple Developer Enterprise Program 的人員), 請先邀請小組成員並指派角色來建置您的小組。若要瞭解如何管理您的小組, 請閱讀 [管理開發人員帳戶小組](#) 的 Apple 檔。

建立 Apple 簽署憑證的步驟

1. 移至 [Apple 開發人員入口網站](#)。
2. 在頁面右上方, 按一下 [帳戶]。
3. 使用 您的組織 Apple ID 登入。
4. 按一下 [憑證]、[設定檔&識別碼] 。



5. 按一下  在右上角新增 iOS 憑證。
6. 選擇在 [生產] 底下建立內部 和臨機****操作 憑證。

 Developer

TechnologiesResourcesProgramsSupportMember Center

Search Developer

Certificates, Identifiers & Profiles

iOS Apps

Certificates

AllPendingDevelopmentProduction

Identifiers

App IDSPass Type IDsWebsite Push IDsiCloud ContainersApp Groups

Devices

All

Provisioning Profiles

AllDevelopmentDistribution

Add iOS Certificate

+

Search

Select TypeRequestGenerateDownload



What type of certificate do you need?

Development

iOS App Development

Sign development versions of your iOS app.

Apple Push Notification service SSL (Sandbox)

Establish connectivity between your notification server and the Apple Push Notification service sandbox environment. A separate certificate is required for each app you develop.

Production

In-House and Ad Hoc

Sign your iOS app for In-House or for Ad Hoc distribution.

MDM CSR

For signing certificate signing requests from MDM solution customers for MDM certificate issuance at [identity.apple.com](#). For more information, read the [Mobile Device Management Protocol Reference](#).

NOTE

如果不打算散發應用程式，而且只想要在內部進行測試，您可以使用 iOS 應用程式開發憑證，而不是生產環境的憑證。如果您使用開發憑證，請確定行動布建設定檔參考將安裝應用程式的裝置。

7. 按一下頁面底部的 [下一步]。

8. 閱讀在 macOS 電腦上使用 Keychain Access 應用程式 (CSR) 建立憑證簽署要求的指示。



About Creating a Certificate Signing Request (CSR)

To manually generate a Certificate, you need a Certificate Signing Request (CSR) file from your Mac. To create a CSR file, follow the instructions below to create one using Keychain Access.

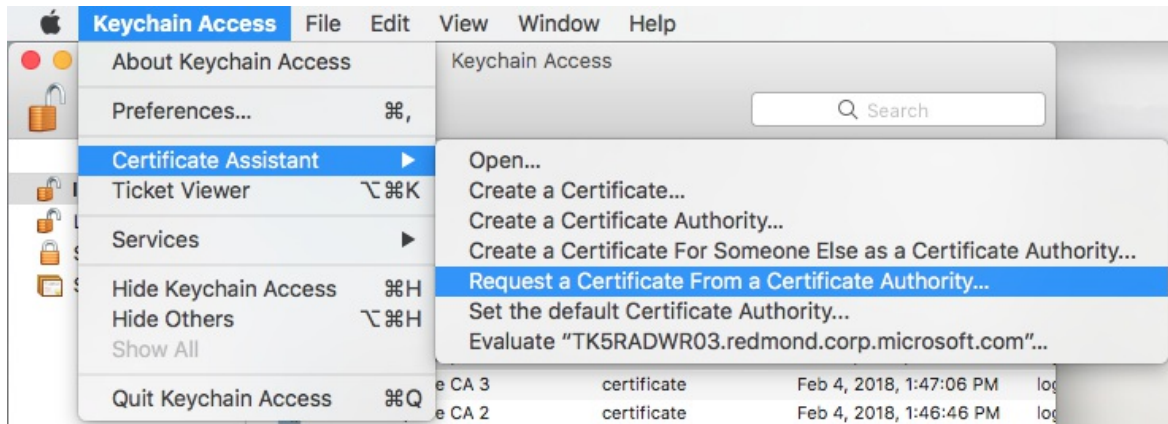
Create a CSR file.

In the Applications folder on your Mac, open the Utilities folder and launch Keychain Access.

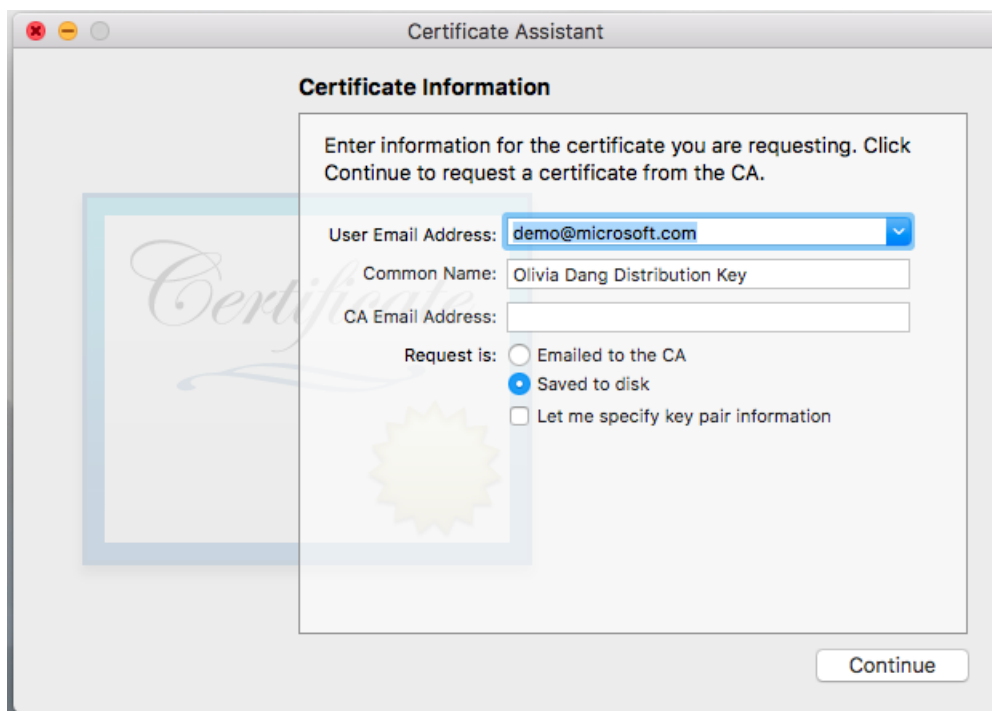
Within the Keychain Access drop down menu, select Keychain Access > Certificate Assistant > Request a Certificate from a Certificate Authority.

- In the Certificate Information window, enter the following information:
 - In the User Email Address field, enter your email address.
 - In the Common Name field, create a name for your private key (e.g., John Doe Dev Key).
 - The CA Email Address field should be left empty.
 - In the "Request is" group, select the "Saved to disk" option.
- Click Continue within Keychain Access to complete the CSR generating process.

9. 請遵循上述指示來建立憑證簽署要求。在 macOS 電腦上，啟動 Keychain Access 應用程式。
10. 在畫面頂端的 macOS 功能表上，移至 [金鑰鏈存取 > 憑證助理 > 向憑證授權單位單位要求憑證]。



11. 請遵循上述 Apple 開發人員網站的指示，瞭解如何建立 CSR 檔案。將 CSR 檔案儲存至 macOS 電腦。



12. 返回 Apple 開發人員網站。按一下 [繼續]。然後上傳 CSR 檔案。
13. Apple 會產生您的簽署憑證。下載並儲存到 macOS 電腦上易記的位置。



Generate your certificate.

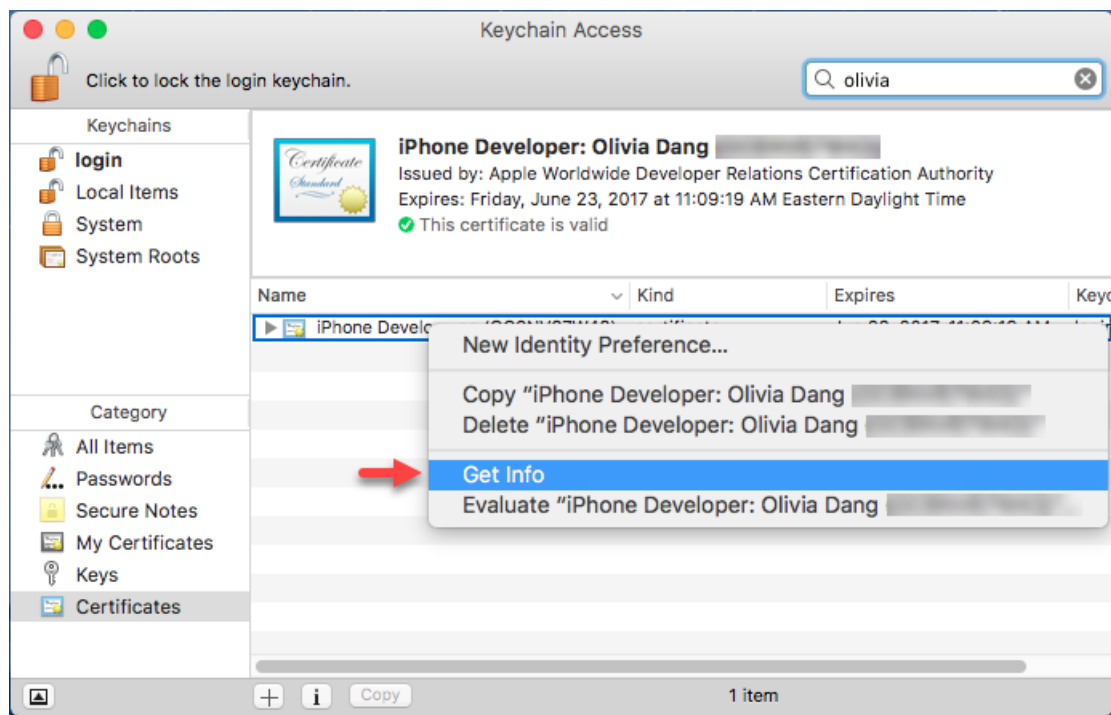
When your CSR file is created, a public and private key pair is automatically generated. Your private key is stored on your computer. On a Mac, it is stored in the login Keychain by default and can be viewed in the Keychain Access app under the "Keys" category. Your requested certificate is the public half of your key pair.

Upload CSR file.

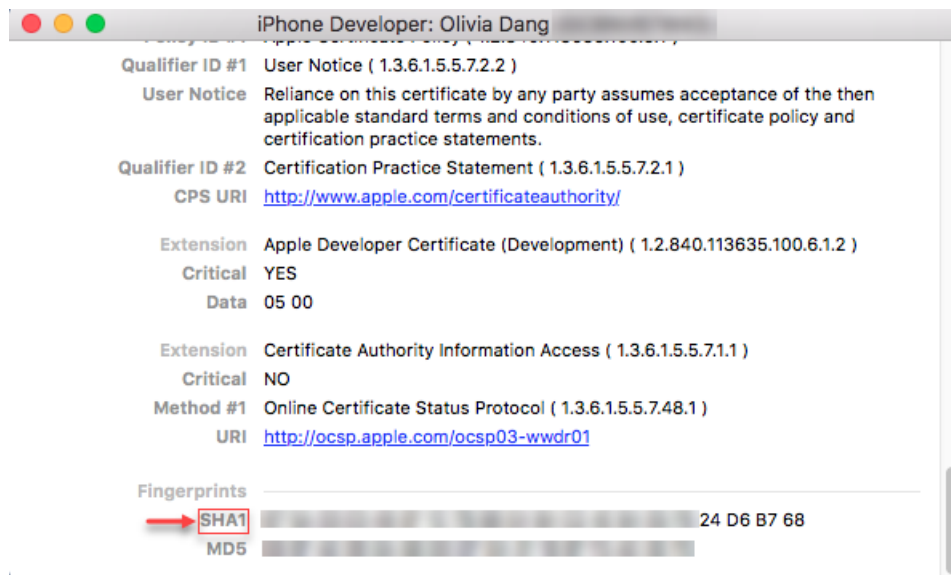
Select .certSigningRequest file saved on your Mac.

Choose File...

14. 按兩下您剛下載的憑證檔案，將憑證新增至金鑰鏈。
15. 再次開啟 [金鑰鏈存取]。在右上方的搜尋列中搜尋憑證的名稱，以找出憑證。以滑鼠右鍵按一下專案以顯示功能表，然後按一下 [取得資訊]。在範例畫面中，我們會使用開發憑證，而不是生產憑證。

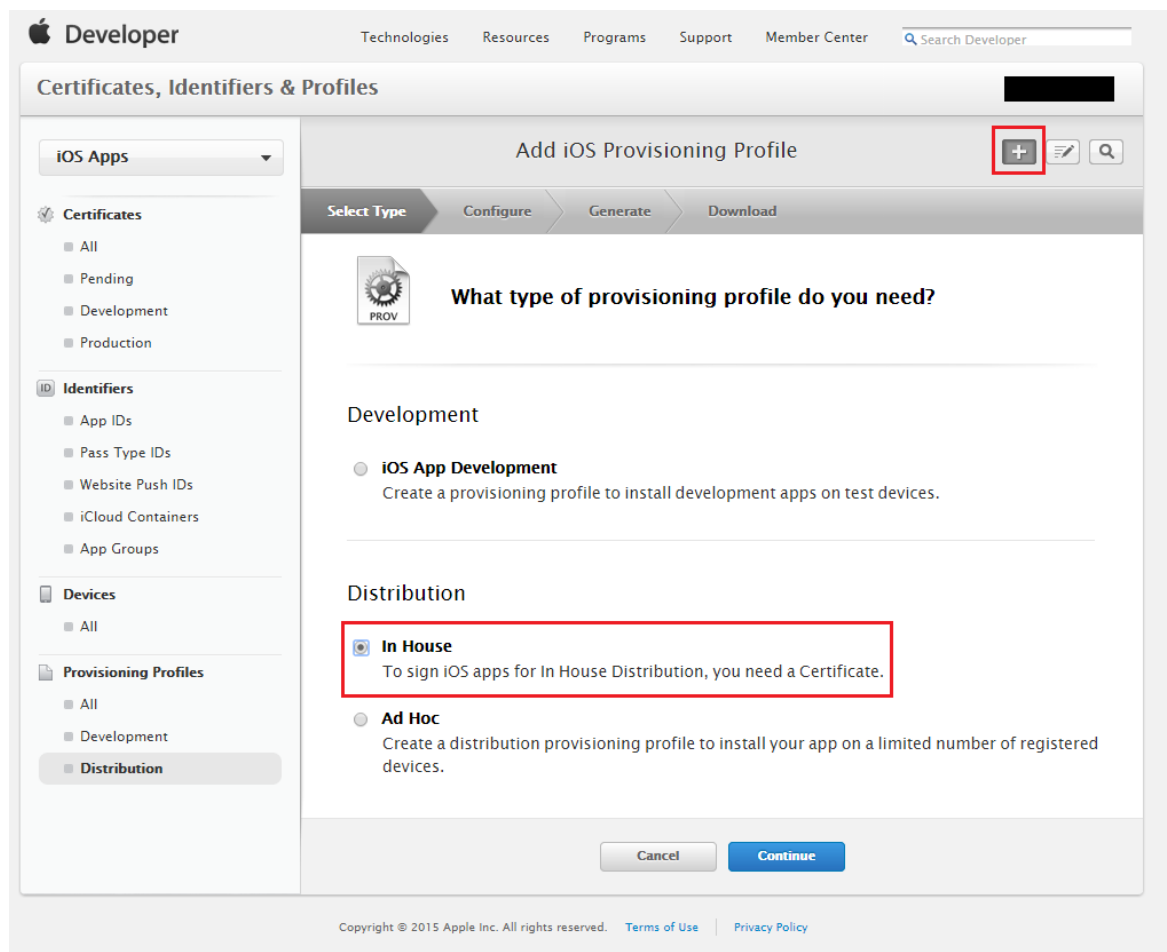


16. 資訊視窗隨即出現。捲動到底部，並查看 [指紋] 卷標下方。將 SHA1 字串複製 (模糊化)，以做為 App Wrapping Tool 「-c」 的引數。



建立In-House散發布建設定檔的步驟

1. 返回至 [Apple Developer 帳戶入口網站](#)，並使用您的組織 Apple ID 登入。
2. 按一下 [憑證]、[設定檔&識別碼]。
3. 按一下  在右上角新增 iOS 布建設定檔。
4. 選擇在 [散發] 底下建立 內部 布建設定檔。



5. 按一下 [繼續]。請務必將先前產生的簽署憑證連結至布建設定檔。
6. 請遵循步驟，將副檔名為 .mobileprovision) 的設定檔 (下載到 macOS 電腦。
7. 將檔案儲存在易記的位置。使用 App Wrapping Tool 時，這個檔案將用於 -p 參數。

下載App Wrapping Tool

1. 將App Wrapping Tool的檔案從[GitHub](#)下載到 macOS 電腦。
2. 按兩下 **Microsoft Intune iOS.dmg 的應用程式限制封裝程式**。隨即會出現具有使用者授權合約 (EULA) 的視窗。請仔細閱讀檔。
3. 選擇 [同意 接受 EULA]，這會將套件掛接至您的電腦。

執行App Wrapping Tool

IMPORTANT

Intune定期發行Intune App Wrapping Tool的更新。定期檢查[iOS 的Intune App Wrapping Tool](#)以取得更新，並併入您的軟體發展發行週期，以確保您的應用程式支援最新的應用程式保護原則設定。

使用終端機

開啟 macOS 終端機，然後執行下列命令：

```
/Volumes/IntuneMAMAppPackager/IntuneMAMPackager/Contents/MacOS/IntuneMAMPackager -i /<path of input app>/<app filename> -o /<path to output folder>/<app filename> -p /<path to provisioning profile> -c <SHA1 hash of the certificate> [-b [<output app build string>]] [-v] [-e] [-x /<array of extension provisioning profile paths>]
```

NOTE

某些參數是選擇性的，如下表所示。

例子：下列範例命令會在名為 MyApp.ipa 的應用程式上執行App Wrapping Tool。系統會指定簽署憑證的布建設定檔和 SHA-1 雜湊，並用來簽署包裝的應用程式。輸出應用程式 (MyApp_Wrapped.ipa) 會建立並儲存在您的 Desktop 資料夾中。

```
./IntuneMAMPackager/Contents/MacOS/IntuneMAMPackager -i ~/Desktop/MyApp.ipa -o ~/Desktop/MyApp_Wrapped.ipa -p ~/Desktop/My_Provisioning_Profile_.mobileprovision -c "12 A3 BC 45 D6 7E F8 90 1A 2B 3C DE F4 AB C5 D6 E7 89 0F AB" -v true
```

命令列參數

您可以使用下列命令列參數搭配App Wrapping Tool：

NOTE

如果您使用 MFA 驗證，則 -aa、-ac 和 -ar 參數不是選擇性的。您必須指定它們，才能允許 MFA 重新導向在登入程式期間運作。

■：下列範例命令會執行App Wrapping Tool，並在驗證程式中使用 MFA 時納入必要的命令。

```
./IntuneMAMPackager/Contents/MacOS/IntuneMAMPackager -i ~/Desktop/MyApp.ipa -o ~/Desktop/MyApp_Wrapped.ipa -p ~/Desktop/My_Provisioning_Profile_.mobileprovision -c "12 A3 BC 45 D6 7E F8 90 1A 2B 3C DE F4 AB C5 D6 E7 89 0F AB" -aa https://login.microsoftonline.com/common -ac "Client ID of the input app if the app uses the Microsoft Authentication Library" -ar "Redirect/Reply URI of the input app if the app uses the Microsoft Authentication Library" -v true
```

[[	]]]]
-i	<code><Path of the input native iOS application file></code> 。檔案名的結尾必須是 .app 或 .ipa。
-o	<code><Path of the wrapped output application></code>
-p	<code><Path of your provisioning profile for iOS apps></code>
-c	<code><SHA1 hash of the signing certificate></code>
-h	顯示有關App Wrapping Tool可用命令列屬性的詳細使用方式資訊。
-aa	(不使用 MFA 時選擇性) <code><Authority URI of the input app if the app uses the Microsoft Authentication Library></code> 也就是 <code>https://login.microsoftonline.com/common</code>
-ac	(未使用 MFA 時為選擇性) <code><Client ID of the input app if the app uses the Microsoft Authentication Library></code> 這是應用程式 [註冊] 刀鋒視窗中應用程式清單中 [用戶端識別碼] 欄位中的 GUID。
-ar	(不使用 MFA 時選擇性) <code><Redirect/Reply URI of the input app if the app uses the Microsoft Authentication Library></code> 這是應用程式註冊中設定的重新導向 URI。一般而言, 這是 Microsoft Authenticator 應用程式在代理驗證之後會傳回的應用程式 URL 通訊協定。
-v	(選擇性) 將詳細資訊訊息輸出至主控台。建議使用此旗標來偵錯任何錯誤。
-e	(選擇性) 使用此旗標可讓App Wrapping Tool在處理應用程式時移除遺漏的權利。如需詳細資訊, 請參閱 設定應用程式權利 。
-xe	(選擇性) 列印應用程式中 iOS 延伸模組的相關資訊, 以及使用它們所需的權利。如需詳細資訊, 請參閱 設定應用程式權利 。
-x	(選擇性) <code><An array of paths to extension provisioning profiles></code> 。如果您的應用程式需要擴充功能布建設定檔, 請使用此功能。
-b	(選擇性) 如果您希望包裝的輸出應用程式具有與輸入應用程式相同的套件組合版本, 請使用 -b, (不建議)。 如果您想要包裝的應用程式具有自訂 CFBundleVersion, 請使用 <code>-b <custom bundle version></code> 。如果您選擇指定自訂 CFBundleVersion, 建議您將原生應用程式的 CFBundleVersion 遞增為最不重要的元件, 例如 1.0.0 -> 1.0.1。

ff	ffff
-f	(選擇性) <Path to a plist file specifying arguments.> 如果您選擇使用 plist 範本來指定其餘的 IntuneMAMPackager 屬性, 例如 -i、-o 和 -p, 請在 plist 檔案前面使用此旗標。請參閱使用 plist 來輸入引數。
-dt	(選擇性) 停用Microsoft Intune用戶端遙測的收集。

使用 plist 輸入引數

執行App Wrapping Tool的簡單方式是將所有命令引數放入[plist](#)檔案。Plist 是類似于 XML 的檔案格式, 可用來使用表單介面輸入命令列引數。

在 IntuneMAMPackager/Contents/MacOS 資料夾中, 使用文字編輯器或 Xcode 開 `Parameters.plist` 啟 (空白 plist 範本)。輸入下列索引鍵的引數:

PLIST 索引鍵	ff	fff	ffff
輸入應用程式封裝路徑	字串	空	與 -i 相同
輸出應用程式封裝路徑	字串	空	與 -o 相同
布建設定檔路徑	字串	空	與 -p 相同
SHA-1 憑證雜湊	字串	空	與 -c 相同
ADAL 授權單位	字串	空	與 -aa 相同
ADAL 用戶端識別碼	字串	空	與 -ac 相同
ADAL 回復 URI	字串	空	與 -ar 相同
已啟用詳細資訊	布林值	假	與 -v 相同
移除遺漏的權利	布林值	假	與 -e 相同
防止預設組建更新	布林值	假	相當於使用 -b 而不使用引數
建置字串覆寫	字串	空	包裝輸出應用程式的自訂 CFBundleVersion
延伸模組布建設定檔路徑	字串陣列	空	應用程式延伸模組布建設定檔的陣列。
停用遙測	布林值	假	與 -dt 相同

以 plist 作為唯一引數來執行 IntuneMAMPackager:

```
./IntuneMAMPackager -f Parameters.plist
```

換行後

包裝程式完成之後，將會顯示「應用程式已成功包裝」訊息。如果發生錯誤，請參閱 [錯誤訊息](#) 以取得說明。

包裝的應用程式會儲存在您先前指定的輸出檔案夾中。您可以將應用程式上傳至 Intune 管理主控台，並將其與行動應用程式管理原則產生關聯。

IMPORTANT

上傳已包裝的應用程式時，如果舊版 (包裝或原生) 版本已部署至 Intune，您可以嘗試更新舊版的應用程式。如果您遇到錯誤，請將應用程式上傳為新的應用程式，並刪除舊版。

您現在可以將應用程式部署到您的使用者群組，並將應用程式保護原則的目標部署至應用程式。應用程式會使用您指定的應用程式保護原則在裝置上執行。

我應該使用 Intune App Wrapping Tool 重寫 iOS 應用程式的頻率為何？

您需要重寫應用程式的主要案例如下：

- 應用程式本身已發行新版本。繼承應用程式已包裝並上傳至 Intune 主控台。
- iOS 的 Intune App Wrapping Tool 已發行新版本，可啟用金鑰錯誤修正或新的特定 Intune 應用程式保護原則功能。這會在 6-8 周之後透過 [適用於 iOS 的 Microsoft Intune App Wrapping Tool](#) GitHub 存放庫發生。

針對 iOS/iPadOS，雖然可以使用與用來簽署應用程式的原始憑證/布建設定檔不同的憑證/布建設定檔來包裝，但如果應用程式中指定的權利未包含在新的布建設定檔中，包裝將會失敗。使用「-e」命令列選項，從應用程式中移除任何遺漏的權利，強制包裝在此案例中不會失敗，可能會導致應用程式的功能中斷。

重新包裝的一些最佳做法包括：

- 確保不同的布建設定檔具有與先前任何布建設定檔一樣的所有必要權利。

錯誤訊息和記錄檔

使用下列資訊，針對應用程式包裝工具的問題進行疑難排解。

錯誤訊息

如果應用程式包裝工具無法順利完成，主控台中會顯示下列其中一個錯誤訊息：

Icon	Message
	您必須指定有效的 iOS 布建設定檔。
	您的布建設定檔可能無效。請檢查以確定您擁有正確的裝置許可權，而且您的設定檔已正確地以開發或散發為目標。您的布建設定檔可能也已過期。
	指定有效的輸入應用程式名稱。
	請確定您指定的輸入應用程式名稱正確無誤。
	指定輸出應用程式的有效路徑。
	請確定您指定的輸出應用程式路徑存在，且正確無誤。
	指定有效的輸入布建設定檔。
	請確定您已提供有效的布建設定檔名稱和延伸模組。您的布建設定檔可能缺少權利，或者您可能未包含 -p 命令列選項。
	找不到您指定的輸入應用程式。指定有效的輸入應用程式名稱和路徑。
	請確定您的輸入應用程式路徑有效且存在。請確定輸入應用程式存在於該位置。
	找不到您指定的輸入布建設定檔。指定有效的輸入布建設定檔。
	請確定輸入布建檔案的路徑有效，而且您指定的檔案存在。

錯誤	說明
找不到您指定的輸出應用程式資料夾。指定輸出應用程式的有效路徑。	請確定您指定的輸出路徑有效且存在。
輸出應用程式沒有 .ipa 副檔名。	只有 .app 和 .ipa 延伸模組的應用程式才會被 App Wrapping Tool 接受。請確定您的輸出檔案具有有效的副檔名。
指定了不正確簽署憑證。指定有效的 Apple 簽署憑證。	請確定您已從 Apple 開發人員入口網站下載正確的簽署憑證。您的憑證可能已過期，或可能遺失公開或私密金鑰。如果您的 Apple 憑證和布建設定檔可用來在 Xcode 內正確簽署應用程式，則它們對 App Wrapping Tool 有效。此外，請確認簽署憑證在主機 macOS 電腦的金鑰鏈內具有唯一的名稱。如果金鑰鏈內有多個相同憑證的版本，則可能會傳回此錯誤。
您指定的輸入應用程式無效。指定有效的應用程式。	請確定您有已編譯為 .app 或 .ipa 檔案的有效 iOS 應用程式。
您指定的輸入應用程式已加密。指定有效的未加密應用程式。	App Wrapping Tool 不支援加密的應用程式。提供未加密的應用程式。
您指定的輸入應用程式不是以位置獨立可執行檔 (PIE 格式) 格式。以 PIE 格式指定有效的應用程式。	位置獨立可執行檔 (PIE) 應用程式可以在執行時于隨機記憶體位址載入。這可以有安全性優點。如需安全性優點的詳細資訊，請參閱您的 Apple Developer 檔。
您指定的輸入應用程式已經包裝。指定有效的未包裝應用程式。	您無法處理已由工具處理的應用程式。如果您想要再次處理應用程式，請使用應用程式的原始版本來執行工具。
您指定的輸入應用程式未簽署。指定有效的已簽署應用程式。	應用程式包裝工具需要簽署應用程式。請參閱您的開發人員檔，以瞭解如何簽署包裝的應用程式。
您指定的輸入應用程式必須是 .ipa 或 .app 格式。	應用程式包裝工具只接受 .app 和 .ipa 延伸模組。請確定您的輸入檔具有有效的副檔名，並已編譯為 .app 或 .ipa 檔案。
您指定的輸入應用程式已經包裝，且位於最新的原則範本版本上。	App Wrapping Tool 不會以最新的原則範本版本來重寫現有的包裝應用程式。
警告：您未指定 SHA1 憑證雜湊。部署之前，請確定已包裝的應用程式已簽署。	請確定您在 -c 命令列旗標之後指定有效的 SHA1 雜湊。

從裝置收集已包裝應用程式的記錄

使用下列步驟，在疑難排解期間取得已包裝應用程式的記錄。

- 移至您裝置上的 iOS 設定應用程式，然後選取您的 LOB 應用程式。
- 選取 [Microsoft Intune]。
- 將 [顯示診斷主控台] 設定切換為 [開啟]。
- 啟動您的 LOB 應用程式。
- 按一下 [開始使用] 連結。
- 您現在可以透過電子郵件共用記錄，或將記錄複製到 OneDrive 位置。

NOTE

使用 Intune App Wrapping Tool 7.1.13 版或更新版本包裝的應用程式會啟用記錄功能。

從系統收集損毀記錄

您的應用程式可能會將有用的資訊記錄到 iOS 用戶端裝置主控台。當您遇到應用程式的問題，而且需要判斷問題是否與App Wrapping Tool或應用程式本身相關時，這項資訊會很有用。若要擷取此資訊，請使用下列步驟：

1. 執行應用程式以重現問題。
2. 依照 Apple 的偵錯已 [部署 iOS 應用程式](#) 指示收集主控台輸出。

包裝的應用程式也會為使用者提供在應用程式當機後透過電子郵件直接從裝置傳送記錄的選項。使用者可以將記錄傳送給您，以視需要檢查並轉寄給 Microsoft。

憑證、布建設定檔和驗證需求

iOS 的App Wrapping Tool有一些必須符合的需求，才能保證完整功能。

“	““““
iOS 布建設定檔	在包含布建設定檔之前，請確定它有效。在處理 iOS 應用程式時，App Wrapping Tool不會檢查布建設定檔是否已過期。如果指定了過期的布建設定檔，應用程式包裝工具將會包含過期的布建設定檔，而且在 iOS 裝置上無法安裝應用程式之前，您不會知道有問題。
iOS 簽署憑證	在您指定簽署憑證之前，請先確定該憑證有效。此工具不會檢查處理 iOS 應用程式時憑證是否已過期。如果提供過期憑證的雜湊，此工具將會處理並簽署應用程式，但無法在裝置上安裝。 請確定為簽署包裝的應用程式所提供的憑證在布建設定檔中具有相符專案。此工具不會驗證布建設定檔是否與為簽署包裝的應用程式所提供的憑證相符。
驗證	裝置必須有 PIN，加密才能運作。在您已部署包裝應用程式的裝置上，觸碰裝置上的狀態列需要使用者使用公司或學校帳戶再次登入。包裝應用程式中的預設原則是在 <i>重新開機時進行驗證</i> 。iOS 會結束應用程式，然後重新開機應用程式，以處理任何外部通知（例如電話）。

設定應用程式權利

包裝您的應用程式之前，您可以授與 [權利](#)，為應用程式提供超出應用程式一般功能的其他許可權和功能。在程式碼簽署期間，會使用 *權利檔案* 來指定應用程式內的特殊許可權（例如，共用金鑰鍵）的存取權。在應用程式開發期間，Xcode 內會啟用稱為 *功能* 的特定應用程式服務。啟用之後，這些功能會反映在您的權利檔案中。如需權利和功能的詳細資訊，請參閱在 iOS 開發人員程式庫中 [新增功能](#)。如需支援功能的完整清單，請參閱 [支援的功能](#)。

適用於 iOS 的App Wrapping Tool支援功能

“	“	““““
應用程式群組	使用應用程式群組允許多個應用程式存取共用容器，並允許應用程式之間的其他處理序間通訊。 若要啟用應用程式群組，請開啟  窗格，然後在  中按一下 。您可以新增應用程式群組或選取現有的群組。	使用應用程式群組時，請使用反向 DNS 標記法： <i>group.com.companyName.AppGroup</i>
背景模式	啟用背景模式可讓您的 iOS 應用程式繼續在背景中執行。	

[[	[[	[[[[[[
資料保護	資料保護會將安全性層級新增至 iOS 應用程式儲存在磁片上的檔案。資料保護會使用存在於特定裝置上的內建加密硬體，將加密格式的檔案儲存在磁片上。您的應用程式必須布建才能使用資料保護。	
應用程式內購買	應用程式內購買可讓您連線到市集，並安全地處理使用者的付款，直接將市集內嵌到您的應用程式中。您可以使用應用程式內購買來收集增強功能的付款，或用於應用程式可用的其他內容。	
金鑰鏈共用	啟用金鑰鏈共用可讓您的應用程式與小組所開發的其他應用程式共用金鑰鏈中的密碼。	使用金鑰鏈共用時，請使用反向 DNS 標記法： <i>com.companyName.KeychainGroup</i>
個人 VPN	啟用個人 VPN 以允許您的應用程式使用網路擴充功能架構建立及控制自訂系統 VPN 設定。	
推播通知	Apple 推播通知服務 (APN) 可讓未在前景執行的代理程式更新使用者它具有使用者的資訊。	若要讓推播通知能夠運作，您必須使用應用程式特定的布建設定檔。 請遵循 Apple 開發人員檔 中的步驟。
無線附屬組態	啟用無線配件組態會將外部配件架構新增至您的專案，並讓您的應用程式設定 MFi Wi-Fi 配件。	

啟用權利的步驟

- 在您的應用程式中啟用功能：
 - 在 Xcode 中，移至您應用程式的目標，然後按一下 [功能]。
 - 開啟適當的功能。如需每個功能以及如何判斷正確值的詳細資訊，請參閱在 iOS 開發人員程式庫中 [新增功能](#)。
 - 請注意您在程式期間建立的任何識別碼。這些也稱為 `AppIdentifierPrefix` 值。
 - 建置並簽署要包裝的應用程式。
- 在布建設定檔中啟用權利：
 - 登入 Apple 開發人員成員中心。
 - 為您的應用程式建立布建設定檔。如需指示，請參閱[如何取得 iOS Intune App Wrapping Tool的必要條件](#)。
 - 在您的布建設定檔中，啟用您在應用程式中擁有的相同權利。您必須 (應用程式開發期間指定的值) 提供相同的標識 `AppIdentifierPrefix` 符。
 - 完成布建設定檔精靈並下載您的檔案。
- 請確定您已滿足所有必要條件，然後包裝應用程式。

針對權利的常見錯誤進行疑難排解

如果 iOS 的 App Wrapping Tool 顯示權利錯誤，請嘗試下列疑難排解步驟。

❗	❗	❗❗❗
無法剖析從輸入應用程式產生的權利。	App Wrapping Tool 無法讀取從應用程式擷取的權利檔案。權利檔案的格式可能不正確。	檢查應用程式的權利檔案。下列指示說明如何這樣做。檢查權利檔案時，請檢查是否有任何格式不正確的語法。檔案應為 XML 格式。
布建設定檔中缺少權利，() 列出遺漏的權利。使用具有這些權利的布建設定檔來重新封裝應用程式。	布建設定檔中啟用的權利與應用程式中啟用的功能不相符。此不相符也適用於與特定功能相關聯的識別碼，(例如應用程式群組和金鑰鏈存取)。	一般而言，您可以建立新的布建設定檔，以啟用與應用程式相同的功能。當設定檔與應用程式之間的識別碼不相符時，App Wrapping Tool 會在可以的情況下取代識別碼。如果您在建立新的布建設定檔之後仍然收到此錯誤，您可以嘗試使用 <code>-e</code> 參數從應用程式移除權利 (請參閱使用 <code>-e</code> 參數從應用程式移除權利一節)。

尋找已簽署應用程式的現有權利

若要檢閱已簽署應用程式和布建設定檔的現有權利：

1. 尋找 .ipa 檔案，並將其副檔名變更為 .zip。
2. 展開 .zip 檔案。這會產生包含 .app 套件組合的 Payload 資料夾。
3. 使用 codesign 工具來檢查 .app 套件組合上的權利，其中 `YourApp.app` 是 .app 套件組合的實際名稱。

```
codesign -d --entitlements :- "Payload/YourApp.app"
```

4. 使用安全性工具來檢查應用程式內嵌布建設定檔的權利，其中 `YourApp.app` 是 .app 套件組合的實際名稱。

```
security cms -D -i "Payload/YourApp.app/embedded.mobileprovision"
```

使用 `-e` 參數從應用程式移除權利

此命令會移除應用程式中不在權利檔案中的任何已啟用功能。如果您移除應用程式所使用的功能，可能會中斷您的應用程式。您可能會移除遺漏功能的範例，是在廠商產生的應用程式中，該應用程式預設具有所有功能。

```
./IntuneMAMPackager/Contents/MacOS/IntuneMAMPackager -i /<path of input app>/<app filename> -o /<path to output folder>/<app filename> -p /<path to provisioning profile> -c <SHA1 hash of the certificate> -e
```

App Wrapping Tool 的安全性和隱私權

當您使用 App Wrapping Tool 時，請使用下列安全性和隱私權最佳做法。

- 您指定的簽署憑證、布建設定檔及企業營運應用程式必須位於您用來執行應用程式包裝工具的相同 macOS 電腦上。如果檔案位於 UNC 路徑上，請確定這些檔案可從 macOS 電腦存取。路徑必須透過 IPsec 或 SMB 簽署來保護。

匯入管理主控台的包裝應用程式應該位於您執行此工具的同一步電腦上。如果檔案位於 UNC 路徑上，請確定該檔案可在執行管理主控台的電腦上存取。路徑必須透過 IPsec 或 SMB 簽署來保護。

- 從 GitHub 存放庫下載 App Wrapping Tool 的環境必須透過 IPsec 或 SMB 簽署來保護。
- 您所處理的應用程式必須來自可信任的來源，以確保防範攻擊。

- 請確定您在App Wrapping Tool中指定的輸出檔案夾受到保護，特別是如果它是遠端資料夾時。
- 包含檔案上傳對話方塊的 iOS 應用程式可讓使用者規避、剪下、複製及貼上套用至應用程式的限制。例如，使用者可以使用 [檔案上傳] 對話方塊來上傳應用程式資料的螢幕擷取畫面。
- 當您從包裝的應用程式中監視裝置上的檔資料夾時，您可能會看到名為 .msftintuneapplaucher 的資料夾。如果您變更或刪除此檔案，可能會影響受限制應用程式的正確運作。

另請參閱

- [決定如何使用 Microsoft Intune 準備應用程式以進行行動應用程式管理](#)
- [裝置原則和設定檔的常見問題、問題和解決方式](#)
- [使用 SDK 啟用應用程式以進行行動應用程式管理](#)

Microsoft Intune App SDK for iOS 開發人員指南

2022/9/27 •

NOTE

請考慮閱讀[開始使用 Intune App SDK 指南](#)一文，其中說明如何準備在每個支援的平臺上進行整合。

若要下載 SDK，請參閱 [下載 SDK 檔案](#)。

如果您在將 Intune App SDK 整合到您的應用程式時遇到問題，請在 GitHub 上提交[協助要求](#)。

Microsoft Intune App SDK for iOS 可讓您將Intune應用程式保護原則 (也稱為應用程式或 MAM 原則) 併入原生 iOS 應用程式中。啟用 MAM 的應用程式是與 Intune App SDK 整合的應用程式。當Intune主動管理應用程式時，IT 系統管理員可以將應用程式保護原則部署到您的行動應用程式。

先決條件

- 您將需要已安裝 Xcode 14.0 或更新版本的 macOS 電腦。
- 您的應用程式必須以 iOS 14.0 或更新版本為目標。
- 檢閱[Intune app SDK for iOS 授權條款](#)。列印並保留記錄的授權條款複本。下載並使用適用於 iOS 的 Intune App SDK，即表示您同意這類授權條款。如果您不接受它們，請勿使用軟體。
- 下載[GitHub](#)上適用於 iOS Intune App SDK 的檔案。

SDK 存放庫中的內容

- **IntuneMAMSwift.xcframework**：Intune App SDK 架構。建議您將此架構連結至應用程式/延伸模組，以啟用Intune用戶端應用程式管理。不過，有些開發人員可能會偏好靜態程式庫的效能優勢。請參閱下列主題：
- **libIntuneMAMSwift.xcframework**：Intune App SDK 靜態程式庫。開發人員可以選擇連結靜態程式庫，而不是架構。由於靜態程式庫會在建置階段直接內嵌到應用程式/延伸模組二進位檔中，因此使用靜態程式庫有一些啟動時間效能優勢。不過，將它整合到您的應用程式是更複雜的程式。如果您的應用程式包含任何延伸模組，將靜態程式庫連結至應用程式和延伸模組會導致較大的應用程式套件組合大小，因為靜態程式庫會內嵌到每個應用程式/延伸模組二進位檔中。使用架構時，應用程式和延伸模組可以共用相同的 Intune SDK 二進位檔，進而產生較小的應用程式大小。
- **IntuneMAMSwiftStub.xcframework**：Intune App SDK Swift Stub 架構。這是 IntuneMAMSwift.xcframework 和 libIntuneMAMSwift.xcframework 的必要相依性，應用程式/擴充功能必須連結。
- **IntuneMAMResources.bundle**：包含 SDK 所依賴資源的資源套件組合。只有整合靜態程式庫 (libIntuneMAMSwift.xcframework) 的應用程式才需要資源套件組合。
- **IntuneMAMConfigurator**：用來設定應用程式或延伸模組 Info.plist 的工具，其中包含Intune管理所需的最小必要變更。根據應用程式或延伸模組的功能，您可能需要對 Info.plist 進行額外的手動變更。

Intune App SDK 的運作方式

Intune App SDK for iOS 的目標是以最少的程式碼變更，將管理功能新增至 iOS 應用程式。程式碼變更的時間越少，上市時間就越少，但不會影響行動應用程式的一致性和穩定性。

將 SDK 建置到您的行動應用程式

IMPORTANT

Intune 定期發行 Intune App SDK 的更新。定期檢查 [Intune App SDK for iOS](#) 是否有更新，並併入您的軟體發展發行週期，以確保您的應用程式支援最新的應用程式保護原則設定。

若要啟用 Intune App SDK，請遵循下列步驟：

1. **選項 1 - 架構 (建議)**：連結 `IntuneMAMSwift.xcframework` 目標和 `IntuneMAMSwiftStub.xcframework` 目標：將 `IntuneMAMSwiftStub.xcframework` 拖 `IntuneMAMSwift.xcframework` 曳至專案目標的 [架構]、[程式庫] 和 [內嵌內容] 清單。

Frameworks, Libraries, and Embedded Content

Name	Embed
 AudioToolbox.framework	Do Not Embed ↕
 CoreServices.framework	Do Not Embed ↕
 ImageIO.framework	Do Not Embed ↕
 IntuneMAMSwift.xcframework	Embed & Sign ↕
 IntuneMAMSwiftStub.xcframework	Embed & Sign ↕
 libc++.tbd	
 libsqlite3.tbd	
 LocalAuthentication.framework	Do Not Embed ↕
 MessageUI.framework	Do Not Embed ↕
 MSAL.xcframework	Embed & Sign ↕
 QuartzCore.framework	Do Not Embed ↕
 Security.framework	Do Not Embed ↕
 SystemConfiguration.framework	Do Not Embed ↕
 WebKit.framework	Do Not Embed ↕
+ —	

NOTE

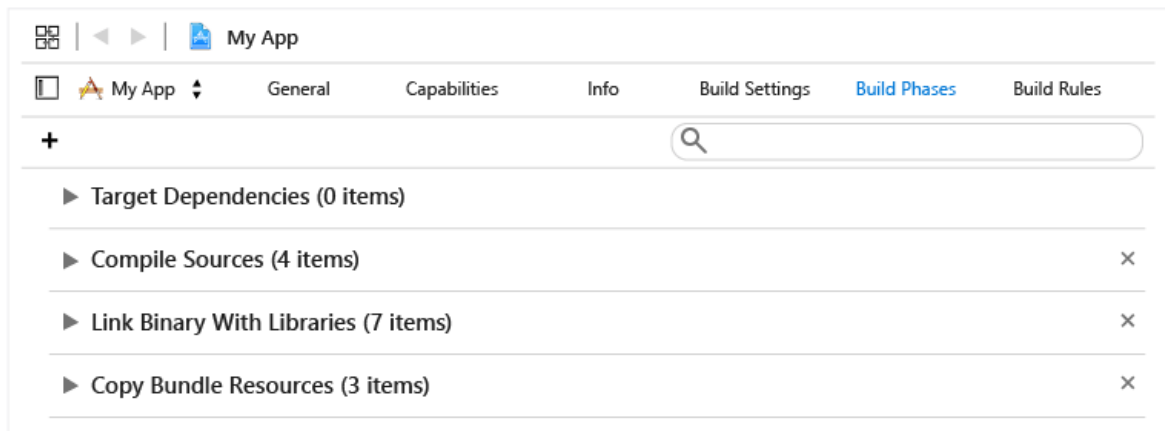
如果您使用 Framework，則必須先手動從通用架構中去除模擬器架構，再將應用程式提交至 App Store。如需詳細資訊，請參閱 [將您的應用程式提交至 App Store](#)。

- 選項 2 - 靜態程式庫**：連結 `libIntuneMAMSwift.xcframework` 和 `IntuneMAMSwiftStub.xcframework` 目標：將 `IntuneMAMSwiftStub.xcframework` 拖 `libIntuneMAMSwift.xcframework` 曳至專案目標的 [架構]、[程式庫] 和 [內嵌內容] 清單。

Frameworks, Libraries, and Embedded Content

Name	Embed
 AudioToolbox.framework	Do Not Embed ↕
 CoreServices.framework	Do Not Embed ↕
 ImageIO.framework	Do Not Embed ↕
 IntuneMAMSwiftStub.xcframework	Embed & Sign ↕
 libc++.tbd	
 libIntuneMAMSwift.xcframework	Embed & Sign ↕
 libsqlite3.tbd	
 LocalAuthentication.framework	Do Not Embed ↕
 MessageUI.framework	Do Not Embed ↕
 MSAL.xcframework	Embed & Sign ↕
 QuartzCore.framework	Do Not Embed ↕
 Security.framework	Do Not Embed ↕
 SystemConfiguration.framework	Do Not Embed ↕
 WebKit.framework	Do Not Embed ↕
+ —	

在建置階段內，`IntuneMAMResources.bundle` 將資源配套拖曳到 [複製 套件組合資源] 底下，將資源配套新增至 專案。



2. 將這些 iOS 架構新增至專案：

- MessageUI.framework
- Security.framework
- CoreServices.framework
- SystemConfiguration.framework
- libsqlite3.tbd
- libc++.tbd
- ImageIO.framework
- LocalAuthentication.framework
- AudioToolbox.framework
- QuartzCore.framework
- WebKit.framework

3. 如果) 尚未啟用金鑰鏈共用 (，請選擇每個專案目標中的 [功能] 並啟用 [金鑰鏈共用] 參數。您必須共用

Keychain, 才能繼續進行下一個步驟。

NOTE

您的布建設定檔需要支援新的金鑰鏈共用值。金鑰鏈存取群組應該支援萬用字元。您可以在文字編輯器中開啟 .mobileprovision 檔案、搜尋 **keychain-access-groups**, 並確保您有萬用字元, 以檢查此情況。例如:

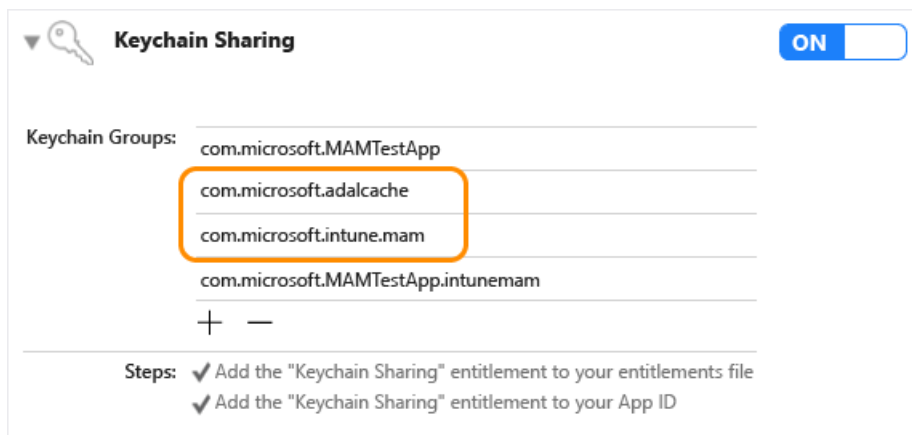
```
<key>keychain-access-groups</key>
<array>
<string>YOURBUNDLESEEDID.*</string>
</array>
```

4. 啟用金鑰鏈共用之後, 請遵循步驟來建立個別的存取群組, Intune App SDK 會在其中儲存其資料。您可以使用 UI 或使用權利檔案來建立金鑰鏈存取群組。如果您使用 UI 來建立金鑰鏈存取群組, 請務必遵循下列步驟:

a. 如果您的行動應用程式未定義任何金鑰鏈存取群組, 請將應用程式的套件組合識別碼新增為 **第一個** 群組。

b. 將共用金鑰鏈群組 `com.microsoft.intune.mam` 新增至現有的存取群組。Intune 應用程式 SDK 會使用此存取群組來儲存資料。

c. 將新 `com.microsoft.adalcache` 增至現有的存取群組。



d. 如果您要直接編輯權利檔案, 而不是使用上面顯示的 Xcode UI 來建立金鑰鏈存取群組, 請在金鑰鏈存取群組 `$(AppIdentifierPrefix)` 前面加上 (Xcode 會自動) 處理此作業。例如:

- `$(AppIdentifierPrefix)com.microsoft.intune.mam`
- `$(AppIdentifierPrefix)com.microsoft.adalcache`

NOTE

權利檔案是行動應用程式唯一的 XML 檔案。它可用來指定 iOS 應用程式中的特殊許可權和功能。如果您的應用程式先前沒有權利檔案, 啟用金鑰鏈共用 (步驟 3) 應該會導致 Xcode 為您的應用程式產生一個金鑰鏈共用。確定應用程式的套件組合識別碼是清單中的第一個專案。

5. 在應用程式的 Info.plist 檔案陣列中包含 `LSApplicationQueriesSchemes` 應用程式傳遞給

`UIApplication canOpenURL` 的每個通訊協定。針對此陣列中所列的每個通訊協定, 附加的通訊協定

`-intunemam` 複本也必須新增至陣列。此外, `http-intunemam`、`https-intunemam`、

`microsoft-edge-http-intunemam`、`microsoft-edge-https-intunemam`、`smart-ns`、`zips`、`wandera`

`lagoonsecurity`、`lookoutwork-ase`、`skycure`、`betteractiveshield`、`smsec`、`mvisionmobile` 和

`scmx` 應該加入至陣列。如果您的應用程式使用 `mailto:` 通訊協定, `ms-outlook-intunemam` 也應該將新增至陣列。請務必先儲存變更, 再繼續進行下一個步驟。

如果應用程式的 `LSApplicationQueriesSchemes` 清單空間不足，則可以移除已知也會實作 Intune MAM SDK 之應用程式的「-intunemam」配置。當應用程式從 `LSApplicationQueriesSchemes` 清單中移除「scheme-intunemam」時，`canOpenURL()` 可能會針對這些配置傳回不正確的回應。若要修正此問題，應用程式應該改為呼叫 `[IntuneMAMPolicy isURLAllowed:url isKnownManagedAppScheme:YES]` 該配置。如果原則將封鎖 URL 的開啟，則此呼叫會傳回 `NO`。如果傳回 `true`，則應用程式可以使用空的身分識別呼叫 `canOpenURL()`，以判斷是否可以開啟 URL。例如：

```
BOOL __block canOpen = NO;
if([policy isURLAllowed:urlForKnownManagedApp isKnownManagedAppScheme:YES])
{
    [[IntuneMAMPolicyManager instance] setCurrentThreadIdentity:@"" forScope:^(
        canOpen = [[UIApplication sharedApplication] canOpenURL:urlForKnownManagedApp];
    )];
}
```

6. 如果您的應用程式尚未使用 FaceID，請確定 [NSFaceIDUsageDescription Info.plist 金鑰](#) 已設定為預設訊息。這是必要專案，讓 iOS 可以讓使用者知道應用程式打算如何使用 FaceID。Intune 應用程式保護原則設定允許在 IT 系統管理員設定時，使用 FaceID 作為應用程式存取的方法。
7. 使用 [SDK 存放庫](#) 中包含的 `IntuneMAMConfigurator` 工具來完成應用程式 `Info.plist` 的設定。此工具有三個參數：

“	““““
- i	<Path to the input plist>
- e	<Path to the entitlements file>
- o	(選擇性) <Path to the output plist>

如果未指定 '-o' 參數，則會就地修改輸入檔。此工具具有等幂性，而且每當對應用程式的 `Info.plist` 或權利進行變更時，都應該重新執行。您也應該在更新 Intune SDK 時下載並執行最新版本的工具，以防 `Info.plist` 組態需求在最新版本中變更。

Xcode 組建設定

應用程式應該同時將「Strip Swift Symbols」(`STRIP_SWIFT_SYMBOLS`) 和「Enable Bitcode」(`ENABLE_BITCODE`) 設定為 `NO`。

整合檔案提供者擴充功能

檔案提供者擴充功能具有某些記憶體需求，可能會讓整合完整的 SDK 變得困難。為了方便起見，有一個靜態程式庫 `libIntuneMAMSwiftFileProvider.xcframework` 是 SDK 的已移除版本，專門用於檔案提供者擴充功能。請注意，這是針對 `FileProvider` 延伸模組的非 UI 部分。您必須將完整的 SDK 整合到檔案提供者 UI 擴充功能。

若要將其中一個程式庫與您的檔案提供者延伸模組整合，請遵循將 SDK 整合為靜態程式庫的步驟，如上所示。請務必包含 `ContainingAppBundleId` 設定。

如果是多重身分識別應用程式，則應該使用 `setIdentity:onFileProviderEnumerator:` 的方法

`IntuneMAMFileProtectionManager`，在 API 的檔案提供者列舉值中 `- enumeratorForContainerItemIdentifier:error:` 設定目前的使用者身分識別。

檢查 `- startProvidingItemAtURL:completionHandler:` 您是否應該使用

`[[IntuneMAMPolicy instance]shouldFileProviderEncryptFiles]]` 來加密檔案。在 中

`IntuneMAMFileProtectionManager` 使用 `encryptFile:forIdentity` API 進行實際檔案加密。此外，在需要加密時共用檔案複本，因為您不想將檔案的加密複本儲存在雲端儲存體中。

在中 `- importDocumentAtURL:toParentItemIdentifier:completionHandler:` 檢查檔案是否使用 `isFileEncrypted:` 中的 API `IntuneMAMFileProtectionManager` 加密。如果是，則使用 `decryptFile:toCopyPath:` 的 `IntuneMAMFileProtectionManager` API 將它解密。

設定 MSAL

Intune 應用程式 SDK 會使用 [Microsoft 驗證程式庫](#) 進行驗證和條件式啟動案例。它也依賴 MSAL 向 MAM 服務註冊使用者身分識別，以便在不使用裝置註冊的情況下進行管理。

設定和設定 AAD 應用程式註冊

MSAL 需要應用程式向 Azure Active Directory (AAD) [註冊](#)，並建立唯一的用戶端識別碼和重新導向 URI，以確保授與應用程式的權杖安全性。如果您的應用程式已經使用 MSAL 進行自己的驗證，則應該已經有與應用程式相關聯的 AAD 應用程式註冊/用戶端識別碼/重新導向 URI。

如果您的應用程式尚未使用 MSAL，您必須在 AAD 中設定應用程式註冊，並指定 Intune SDK 應該使用的用戶端識別碼和重新導向 URI。

如果您的應用程式目前使用 ADAL 來驗證使用者，請參閱將 [應用程式移轉至適用於 iOS 和 macOS 的 MSAL](#)，以取得將應用程式從 ADAL 移轉至 MSAL 的詳細資訊。

建議您的應用程式連結至最新版本的 [MSAL](#)。

將 MSAL 連結至您的專案

請遵循 [安裝](#) 一節，將 MSAL 二進位檔放在您的應用程式中。

設定 MSAL

請遵循組態一節來設定 MSAL。請務必遵循組態一節中的所有步驟。如果您的應用程式已在 AAD 中註冊，請忽略步驟一。

下列各點包含設定 MSAL 並連結至該處的其他資訊。如果套用至您的應用程式，請遵循這些程式碼。

- 如果您的應用程式未定義任何金鑰鏈存取群組，請將應用程式的套件組合識別碼新增為第一個群組。
- 將新增至金鑰鏈存取群組，以啟用 MSAL 單一登入 (SSO) `com.microsoft.adalcache`。
- 如果您要明確設定 MSAL 共用快取金鑰鏈群組，請確定它已設定為 `<appidprefix>.com.microsoft.adalcache`。MSAL 會為您設定此專案，除非您覆寫它。如果您想要指定要取代 `com.microsoft.adalcache` 的自訂 keychain 群組，請使用金鑰 `ADALCacheKeychainGroupOverride`，在 IntuneMAMSettings 下的 Info.plist 檔案中指定。

設定 Intune App SDK 的 MSAL 設定

在 AAD 中為您的應用程式設定應用程式註冊之後，您可以設定 Intune App SDK，以便在對 AAD 進行驗證期間使用來自應用程式註冊的設定。如需填入下列設定的資訊，請參閱設定 [Intune App SDK](#) 的設定：

- ADALClientId
- ADALAuthority
- ADALRedirectUri
- ADALRedirectScheme
- ADALCacheKeychainGroupOverride

需要下列設定：

- 在專案的 Info.plist 檔案中，于具有索引鍵名稱 `ADALClientId` 的 IntuneMAMSettings 字典底下，指定要用於 MSAL 呼叫的用戶端識別碼。
- 如果對應至步驟 1 中所設定之用戶端識別碼的 Azure AD 應用程式註冊設定為只在單一 AAD 租使用者中使用，`ADALAuthority` 請在應用程式 Info.plist 檔案內的 IntuneMAMSettings 字典下設定金鑰。指定 MSAL 要用來取得 Intune 行動應用程式管理服務權杖的 Azure AD 授權單位。

3. 此外，在具有索引鍵名稱 `ADALRedirectUri` 的 `IntuneMAMSettings` 字典下，指定要用於 MSAL 呼叫的重新導向 URI。或者，如果應用程式的重新導向 URI 格式 `scheme://bundle_id` 為，您可以改為指定 `ADALRedirectScheme`。

或者，應用程式可以在執行時間覆寫這些 Azure AD 設定。若要這樣做，只要在類別上 `IntuneMAMSettings` 設定 `aadAuthorityUriOverride`、`aadClientIdOverride` 和 `aadRedirectUriOverride` 屬性即可。

4. 請確定已遵循將 iOS 應用程式許可權授與應用程式保護原則 (APP) 服務的步驟。請使用開始[使用Intune SDK 指南](#)中的指示，在「[將應用程式存取權授與Intune應用程式保護服務 \(選擇性\)](#)」之下。

NOTE

建議針對靜態且不需要在執行時間決定的所有設定使用 Info.plist 方法。在執行時間指派給類別屬性的 `IntuneMAMSettings` 值會優先於 Info.plist 中指定的任何對應值，而且即使在應用程式重新開機之後仍會保存。SDK 會繼續將它們用於原則簽入，直到使用者取消註冊或清除或變更值為止。

使用 MSAL 進行應用程式起始驗證時的特殊考慮

建議應用程式不要使用 `SFSafariViewController`、`SFAuthenticationSession` 或 `ASWebAuthenticationSession` 作為任何應用程式起始 MSAL 互動式驗證作業的 Web 檢視。根據預設，MSAL 會使用 `ASWebAuthenticationSession`，因此應用程式開發人員應該 [明確地將 Web 檢視類型設定](#) 為 `WKWebView`。如果因為某些原因，您的應用程式必須針對任何互動式 MSAL 驗證作業使用 `WKWebView` 以外的 Web 檢視類型，則它也必須在應用程式 Info.plist 的字典底下 `IntuneMAMSettings` 設定為 `SafariViewControllerBlockedOverride` `true`。警告：這會關閉Intune的 `SafariViewController` 勾點，以啟用驗證會話。如果應用程式使用 `SafariViewController` 來檢視公司資料，這會造成應用程式中其他位置的資料外泄的風險，因此應用程式不應該在其中任何一種 Web 檢視類型中顯示公司資料。

設定 Intune App SDK 的設定

您可以在應用程式的 Info.plist 檔案中使用 `IntuneMAMSettings` 字典來設定 Intune App SDK。如果 Info.plist 檔案中看不到 `IntuneMAMSettings` 字典，您應該建立它。

在 `IntuneMAMSettings` 字典下，您可以定義下列支援的設定，以設定 Intune App SDK。

上述部分設定可能已涵蓋在先前的章節中，有些則不適用於所有應用程式。

「	「	「	「?
<code>ADALClientId</code>	字串	應用程式的 Azure AD 用戶端識別碼。	所有使用 MSAL 的應用程式皆為必要專案。
<code>ADALAuthority</code>	字串	應用程式的 Azure AD 授權單位正在使用中。您應該使用已設定 AAD 帳戶的專屬環境。如需詳細資訊，請參閱 應用程式組態選項 。	如果應用程式是專為在單一組織/AAD 租使用者內使用而建置的自訂企業營運應用程式，則為必要專案。如果此值不存在，則會使用通用 AAD 授權單位 (只支援多租使用者應用程式)。
<code>ADALRedirectUri</code>	字串	應用程式的 Azure AD 重新導向 URI。	所有使用 MSAL 的應用程式，以及任何存取非Intune AAD 資源的 ADAL 應用程式，都需要 <code>ADALRedirectUri</code> 或 <code>ADALRedirectScheme</code> 。

⌘	⌘	⌘	⌘?
ADALRedirectScheme	字串	應用程式的 Azure AD 重新導向配置。如果應用程式的重新導向 URI 格式 <code>scheme://bundle_id</code> 為，這可以用來取代 ADALRedirectUri。	所有使用 MSAL 的應用程式，以及任何存取非Intune AAD 資源的 ADAL 應用程式，都需要 ADALRedirectUri 或 ADALRedirectScheme。
ADALLogOverrideDisabled	布林值	指定如果有任何 MSAL 記錄檔)，SDK 是否會將所有 MSAL 記錄路由 (包括來自應用程式的 MSAL 呼叫。預設為 NO。如果應用程式將設定自己的 MSAL 記錄回呼，請設定為 [是]。	選用。
ADALCacheKeychainGroupOverride	字串	指定要用於 MSAL 快取的 Keychain 群組，而不是「com.microsoft.adalcache」。請注意，這沒有 app-id 前置詞。這會在執行時間前置詞為提供的字串。	選用。
AppGroupIdentifiers	字串陣列	應用程式權利 com.apple.security.application-groups 區段中的應用程式群組陣列。	如果應用程式使用應用程式群組，則為必要專案。
ContainingAppBundleId	字串	指定延伸模組包含應用程式的套件組合識別碼。	iOS 擴充功能的必要專案。
DebugSettingsEnabled	布林值	如果設定為 [是]，則可以套用 [設定] 套件組合內的測試原則。 <i>應用程式不應該</i> 隨附啟用此設定。	選用。預設為否。
AutoEnrollOnLaunch	布林值	指定如果偵測到現有的受控識別且尚未註冊，應用程式是否應該在啟動時嘗試自動註冊。預設為 NO。 注意：如果找不到受控識別，或 MSAL 快取中沒有可用的身分識別有效權杖，註冊嘗試將會以無訊息方式失敗，而不會提示輸入認證，除非應用程式也已將 MAMPolicyRequired 設定為 YES。	選用。預設為否。

名稱	類型	說明	預設值
MAMPolicyRequired	布林值	指定如果應用程式沒有 Intune 應用程式保護原則，是否會封鎖應用程式啟動。 預設為 NO。 附注：應用程式無法提交至 MAMPolicyRequired 設為 YES 的 App Store。將 MAMPolicyRequired 設定為 YES 時，AutoEnrollOnLaunch 也應該設定為 YES。	選用。預設為否。
MAMPolicyWarnAbsent	布林值	指定如果應用程式沒有應用程式保護原則，應用程式是否會在啟動期間警告使用者 Intune。 注意：關閉警告之後，仍然允許使用者在沒有原則的情況下使用應用程式。	選用。預設為否。
Multitendancy	布林值	指定應用程式是否為多重身分識別感知。	選用。預設為否。
SafariViewControllerBlockedOverride	布林值	停用 Intune 的 SafariViewController 勾點，以透過 SFSafariViewController、SFAuthSession 或 ASWebAuthenticationSession 啟用 MSAL 驗證。 注意：Intune 的受控 Safari 檢視控制器不支援 SFSafariViewControllerConfiguration 活動按鈕屬性。只有在檢視未受管理且 SafariViewControllerBlockedOverride 設定為 [是] 時，設定 的活動按鈕 才會出現在 SafariViewController 中。	選用。預設為否。警告：如果使用不當，可能會導致資料外泄。只有在絕對必要時才啟用。如需詳細資訊，請參閱 使用 MSAL 進行應用程式起始驗證時的特殊考慮 。
SplashIconFile SplashIconFile~ipad	字串	指定啟動) 圖示檔案 (Intune 啟動)。	選用。
SplashDuration	數字	Intune 啟動畫面在應用程式啟動時顯示的最小時間量，以秒為單位。預設為 1.5。	選用。
BackgroundColor	字串	指定 Intune SDK UI 元件的背景色彩。以 #XXXXXX 的形式接受十六進位 RGB 字串，其中 X 的範圍可以是 0-9 或 A-F。可能會省略井字型大小。	選用。預設為系統背景色彩，這可能會因 iOS 版本和 iOS 深色模式設定而有所不同。

名稱	類型	說明	預設值
ForegroundColor	字串	指定Intune SDK UI 元件的前景色彩，例如文字色彩。以#XXXXXX的形式接受十六進位 RGB 字串，其中 X 的範圍可以是 0-9 或 A-F。可能會省略井字型大小。	選用。預設為系統磁碟區標色彩，可能會因 iOS 版本和 iOS 深色模式設定而有所不同。
AccentColor	字串	指定Intune SDK UI 元件的輔色，例如按鈕文字色彩和 PIN 方塊醒目提示色彩。以#XXXXXX的形式接受十六進位 RGB 字串，其中 X 的範圍可以是 0-9 或 A-F。可能會省略井字型大小。	選用。預設為系統藍色。
SecondaryBackgroundColor	字串	指定 MTD 畫面的次要背景色彩。以#XXXXXX的形式接受十六進位 RGB 字串，其中 X 的範圍可以是 0-9 或 A-F。可能會省略井字型大小。	選用。預設為白色。
SecondaryForegroundColor	字串	指定 MTD 畫面的次要前景色彩，例如註腳色彩。以#XXXXXX的形式接受十六進位 RGB 字串，其中 X 的範圍可以是 0-9 或 A-F。可能會省略井字型大小。	選用。預設為灰色。
SupportsDarkMode	布林值	指定如果未針對 BackgroundColor/ForegroundColor/AccentColor 設定明確的值，Intune SDK 的 UI 色彩配置是否應該觀察系統深色模式設定	選用。預設為 [是]。
MAMTelemetryDisabled	布林值	指定 SDK 是否會將任何遙測資料傳送至其後端。	選用。預設為否。
MAMTelemetryUsePPE	布林值	指定 MAM SDK 是否會將資料傳送至 PPE 遙測後端。使用Intune原則測試您的應用程式時，請使用此方法，讓測試遙測資料不會與客戶資料混用。	選用。預設為否。

名稱	類型	說明	預設值
MaxFileProtectionLevel	字串	允許應用程式指定可支援的最大 <code>NSFileProtectionType</code> 值。如果層級高於應用程式可支援的層級，這個值將會覆寫服務所傳送的原則。可能的值： <code>NSFileProtectionComplete</code> 、 <code>NSFileProtectionCompleteUnlessOpen</code> 、 <code>NSFileProtectionCompleteUntilFirstUserAuthentication</code> 、 <code>NSFileProtectionNone</code> 。 注意：使用最高的檔案保護層級 (<code>NSFileProtectionComplete</code>)，受保護的檔案只能在裝置解除鎖定時存取。裝置鎖定後 10 秒，應用程式將失去受保護檔案的存取權。	選用。預設為 <code>NSFileProtectionComplete</code> 。
OpenInActionExtension	布林值	針對 [在動作中開啟] 延伸模組，設定為 [是]。如需詳細資訊，請參閱透過 <code>UIActivityViewController</code> 共用資料一節。	
WebViewHandledURLSchemes	字串陣列	指定您應用程式的 <code>WebView</code> 處理的 URL 配置。	如果您的應用程式使用可透過連結和/或 JavaScript 處理 URL 的 <code>WebView</code> ，則為必要專案。
DocumentBrowserFileCachePath	字串	如果您的應用程式使用 <code>UIDocumentBrowserViewController</code> 來流覽各種檔案提供者中的檔案，您可以設定此路徑相對於應用程式沙箱中的主目錄，讓 Intune SDK 可以將解密的受控檔案放入該資料夾。	選用。預設為 <code>/Documents/</code> 目錄。
VerboseLoggingEnabled	布林值	如果設定為 [是]，Intune 會以詳細資訊模式登入。	選用。預設為 NO
FinishLaunchingAtStartup	布林值	如果應用程式正在使用 <code>[BGTaskScheduler registerForTaskWithIdentifier:]</code> ，則此設定應該設定為 YES。	選用。預設為 NO

接收應用程式保護原則

概觀

若要接收 Intune 應用程式保護原則，應用程式必須向 Intune MAM 服務起始註冊要求。您可以在 Intune 主控台中設定應用程式，以接收具有或不註冊裝置的應用程式保護原則。[行動應用程式管理 \(MAM\)](#)，可讓應用程式由 Intune 管理，而不需要在 Intune 行動裝置管理 (MDM) 中註冊裝置。在這兩種情況下，必須向 Intune MAM 服務註冊才能接收原則。

IMPORTANT

Intune App SDK for iOS 會在應用程式保護原則啟用加密時使用 256 位加密金鑰。所有應用程式都必須有目前的 SDK 版本，才能允許受保護的資料共用。

已使用 ADAL 或 MSAL 的應用程式

NOTE

Azure Active Directory (Azure AD) 驗證程式庫 (ADAL) 和 Azure AD 圖形 API 將會被取代。如需詳細資訊，請參閱[更新您的應用程式以使用 Microsoft 驗證程式庫 \(MSAL\) 和 Microsoft 圖形 API](#)。

已使用 ADAL 或 MSAL 的應用程式應該在使用者成功驗證之後，于實例上 `IntuneMAMEnrollmentManager` 呼叫 `registerAndEnrollAccount` 方法：

```
/*
 * This method will add the account to the list of registered accounts.
 * An enrollment request will immediately be started.
 * @param identity The UPN of the account to be registered with the SDK
 */

(void)registerAndEnrollAccount:(NSString *)identity;
```

藉由呼叫 `registerAndEnrollAccount` 方法，SDK 將會註冊使用者帳戶，並嘗試代表此帳戶註冊應用程式。如果註冊因為任何原因而失敗，SDK 會在 24 小時後自動重試註冊。基於偵錯目的，應用程式可以透過委派接收有關任何註冊要求結果的[通知](#)。

叫用此 API 之後，應用程式可以繼續正常運作。如果註冊成功，SDK 會通知使用者需要重新開機應用程式。屆時，使用者可以立即重新開機應用程式。

```
[[IntuneMAMEnrollmentManager instance] registerAndEnrollAccount:@"user@foo.com"];
```

不使用 ADAL 或 MSAL 的應用程式

未使用 ADAL 或 MSAL 登入使用者的應用程式仍可藉由呼叫 API 讓 SDK 處理該驗證，從 Intune MAM 服務接收應用程式保護原則。當應用程式尚未向 Azure AD 驗證使用者，但仍需要擷取應用程式保護原則來協助保護資料時，應該使用這項技術。例如，如果另一個驗證服務用於應用程式登入，或應用程式完全不支援登入。若要這樣做，應用程式可以在實例上 `IntuneMAMEnrollmentManager` 呼叫 `loginAndEnrollAccount` 方法：

```
/**
 * Creates an enrollment request which is started immediately.
 * If no token can be retrieved for the identity, the user will be prompted
 * to enter their credentials, after which enrollment will be retried.
 * @param identity The UPN of the account to be logged in and enrolled.
 */

(void)loginAndEnrollAccount: (NSString *)identity;
```

藉由呼叫這個方法，如果找不到現有的權杖，SDK 會提示使用者輸入認證。然後，SDK 會嘗試代表提供的使用者帳戶向 Intune MAM 服務註冊應用程式。方法可以使用「nil」做為身分識別來呼叫。在此情況下，SDK 會在 MDM 的情況下，向裝置 (上現有的受控使用者註冊，如果找不到現有的使用者，則提示使用者輸入使用者名稱。

如果註冊失敗，應用程式應該考慮在未來再次呼叫此 API，視失敗的詳細資料而定。應用程式可以透過委派接收有關任何註冊要求結果的[通知](#)。

叫用此 API 之後，應用程式可以繼續正常運作。如果註冊成功，SDK 會通知使用者需要重新開機應用程式。

範例：

```
[[IntuneMAMEnrollmentManager instance] loginAndEnrollAccount:@"user@foo.com"];
```

讓 Intune 在啟動時處理驗證和註冊

如果您希望 Intune SDK 在應用程式啟動完成之前，先使用 ADAL/MSAL 和註冊來處理所有驗證，而且您的應用程式一律需要 APP 原則，則不需要使用 `loginAndEnrollAccount` API。在應用程式 Info.plist 的 IntuneMAMSettings 字典中，您可以直接將下列兩個設定設定為 [是]。

名稱	類型	說明
AutoEnrollOnLaunch	布林值	指定如果偵測到現有的受控識別且尚未註冊，應用程式是否應該在啟動時嘗試自動註冊。預設為 NO。 注意：如果找不到受控識別，或 ADAL/MSAL 快取中沒有可用的身分識別有效權杖，註冊嘗試將會以無訊息方式失敗，而不會提示輸入認證，除非應用程式也已將 MAMPolicyRequired 設定為 YES。
MAMPolicyRequired	布林值	指定如果應用程式沒有 Intune 應用程式保護原則，是否會封鎖應用程式啟動。預設為 NO。 注意：無法將 MAMPolicyRequired 設定為 YES 的應用程式提交至 App Store。將 MAMPolicyRequired 設定為 YES 時，AutoEnrollOnLaunch 也應該設定為 YES。

如果您為應用程式選擇此選項，則不需要在註冊之後處理重新開機應用程式。

取消註冊使用者帳戶

在使用者登出應用程式之前，應用程式應該先從 SDK 取消註冊使用者。這可確保：

1. 使用者的帳戶不會再進行註冊重試。
2. 將會移除應用程式防護原則。
3. 如果應用程式起始選擇性抹除 (選擇性)，則會刪除任何公司資料。

在使用者登出之前，應用程式應該在 [實例上](#) `IntuneMAMEnrollmentManager` 呼叫下列方法：

```
/*
 * This method will remove the provided account from the list of
 * registered accounts. Once removed, if the account has enrolled
 * the application, the account will be un-enrolled.
 * @note In the case where an un-enroll is required, this method will block
 * until the Intune APP AAD token is acquired, then return. This method must be called before
 * the user is removed from the application (so that required AAD tokens are not purged
 * before this method is called).
 * @param identity The UPN of the account to be removed.
 * @param doWipe If YES, a selective wipe if the account is un-enrolled
 */
(void)deRegisterAndUnenrollAccount:(NSString *)identity withWipe:(BOOL)doWipe;
```

在刪除使用者帳戶的 Azure AD 權杖之前，必須先呼叫此方法。SDK 需要使用者帳戶的 AAD 權杖 ()，才能代表

使用者對Intune MAM 服務提出特定要求。

如果應用程式將自行刪除使用者的公司資料，`doWipe` 則旗標可以設定為 `false`。否則，應用程式可以讓 SDK 起始選擇性抹除。這會導致呼叫應用程式的選擇性抹除委派。

範例：

```
[[IntuneMAMEnrollmentManager instance] deRegisterAndUnenrollAccount:@"user@foo.com" withWipe:YES];
```

狀態、結果和偵錯通知

應用程式可以接收下列對 Intune MAM 服務要求的狀態、結果和偵錯通知：

- 註冊要求
- 原則更新要求
- 取消註冊要求

通知是透過 中的委派方法 `IntuneMAMEnrollmentDelegate.h` 來呈現：

```
/**
 * Called when an enrollment request operation is completed.
 * @param status status object containing debug information
 */
(void)enrollmentRequestWithStatus:(IntuneMAMEnrollmentStatus *)status;

/**
 * Called when a MAM policy request operation is completed.
 * @param status status object containing debug information
 */
(void)policyRequestWithStatus:(IntuneMAMEnrollmentStatus *)status;

/**
 * Called when a un-enroll request operation is completed.
 * @Note: when a user is un-enrolled, the user is also de-registered with the SDK
 * @param status status object containing debug information
 */
(void)unenrollRequestWithStatus:(IntuneMAMEnrollmentStatus *)status;
```

這些委派方法會傳 `IntuneMAMEnrollmentStatus` 回具有下列資訊的物件：

- 與要求相關聯之帳戶的身分識別
- 狀態碼，指出要求的結果
- 具有狀態碼描述的錯誤字串
- `NSError` 物件。這個物件定義于 `IntuneMAMEnrollmentStatus.h`，以及可傳回的特定狀態碼。

範例程式碼

以下是委派方法的範例實作：

```

- (void)enrollmentRequestWithStatus:(IntuneMAMEnrollmentStatus*)status
{
    NSLog(@"enrollment result for identity %@ with status code %ld", status.identity, (unsigned long)status.statusCode);
    NSLog(@"Debug Message: %@", status.errorString);
}

- (void)policyRequestWithStatus:(IntuneMAMEnrollmentStatus*)status
{
    NSLog(@"policy check-in result for identity %@ with status code %ld", status.identity, (unsigned long)status.statusCode);
    NSLog(@"Debug Message: %@", status.errorString);
}

- (void)unenrollRequestWithStatus:(IntuneMAMEnrollmentStatus*)status
{
    NSLog(@"un-enroll result for identity %@ with status code %ld", status.identity, (unsigned long)status.statusCode);
    NSLog(@"Debug Message: %@", status.errorString);
}

```

應用程式重新開機

當應用程式第一次收到 MAM 原則時，必須重新開機才能套用必要的勾點。若要通知應用程式需要重新開機，SDK 會在 `IntuneMAMPolicyDelegate.h` 中提供委派方法。

```

- (BOOL) restartApplication

```

這個方法的傳回值會告知 SDK 應用程式是否必須處理必要的重新開機：

- 如果傳回 true，應用程式必須處理重新開機。
- 如果傳回 false，SDK 會在此方法傳回之後重新開機應用程式。SDK 會立即顯示對話方塊，告知使用者重新開機應用程式。

使用 API 自訂應用程式的行為

Intune App SDK 有數個 API 可供您呼叫，以取得部署至應用程式Intune應用程式原則的相關資訊。您可以使用此資料來自訂應用程式的行為。下表提供您將使用之一些基本Intune類別的相關資訊。

「	「
IntuneMAMPolicyManager.h	IntuneMAMPolicyManager 類別會公開部署至應用程式的 Intune 應用程式原則。值得注意的是，它會公開適用於 啟用多重身分識別 的 API。
IntuneMAMPolicy.h	IntuneMAMPolicy 類別會公開一些套用至應用程式的 MAM 原則設定。這些原則設定大部分都會公開，讓應用程式可以自訂其 UI。大部分的原則設定都是由 SDK 強制執行，而不是由應用程式強制執行。不過，有一些例外狀況。應用程式開發人員應該檢閱此標頭中的批註，以判斷哪些 API 適用於其應用程式的案例。
IntuneMAMFileProtectionManager.h	IntuneMAMFileProtectionManager 類別會公開應用程式可用來根據提供的身分識別明確保護檔案和目錄的 API。身分識別可由 Intune 或 Unmanaged 管理，而 SDK 會套用適當的 MAM 原則。使用這個類別是選擇性的。

“	“
IntuneMAMDataProtectionManager.h	IntuneMAMDataProtectionManager 類別會公開應用程式在提供身分識別時可用來保護資料緩衝區的 API。身分識別可以由Intune或 Unmanaged 管理, 而 SDK 會適當地套用加密。

實作允許的帳戶

Intune可讓 IT 系統管理員指定使用者可以登入哪些帳戶。應用程式可以查詢 Intune App SDK 中指定的允許帳戶清單, 然後確定只允許的帳戶登入裝置。

若要查詢允許的帳戶, 應用程式應該檢查 `allowedAccounts` 上的 `IntuneMAMEnrollmentManager` 屬性。屬性 `allowedAccounts` 是包含允許帳戶的陣列或 `nil`。如果屬性為 `nil`, 則未指定任何允許的帳戶。

應用程式也可以藉由觀察通知來回應屬性的 `IntuneMAMAllowedAccountsDidChangeNotification` 變更 `allowedAccounts`。每當 屬性值變更時, `allowedAccounts` 就會張貼通知。

實作所需的檔案加密

`isFileEncryptionRequired` 當 IT 系統管理員要求應用程式在儲存至磁片的任何檔案上使用Intune加密時, 中定義的 `IntuneMAMPolicy.h` API 會通知應用程式。如果 `isFileEncryptionRequired` 為 `true`, 則應用程式必須負責確保應用程式儲存到磁片的任何檔案都會使用 `IntuneMAMFileProtectionManager.h` 和 `IntuneMAMFDataProtectionManager.h` 中的 `IntuneMAMFile.h` API 進行加密。

應用程式可以觀察 中定義的通知, `IntuneMAMDataProtectionDidChangeNotification` 以回應此原則中的 `IntuneMAMFDataProtectionManager.h` 變更。

實作另存新檔和開啟控制項

Intune可讓 IT 系統管理員選取受控應用程式可將資料儲存至或開啟資料的儲存位置。應用程式可以使用 `isSaveToAllowedForLocation:withAccount:` 中定義 `IntuneMAMPolicy.h` 的 API, 查詢 Intune MAM SDK 以取得允許的儲存至儲存體位置。應用程式也可以使用 `isOpenFromAllowedForLocation:withAccount:` 中定義的 API, 查詢 SDK 中 `IntuneMAMPolicy.h` 允許的從儲存體位置開啟。

此外, 應用程式可以查詢 中 `IntuneMAMPolicy.h` 定義的 API, 以確認允許來自共用擴充功能的 `canReceiveSharedItemProvider:` 傳入資料。應用程式也可以查詢 `canReceiveSharedFile:` API, 以驗證來自 `openURL` 呼叫的連入檔案, 也定義于 `IntuneMAMPolicy.h`

NOTE

自 MAM SDK v15.1.0 起, 已對內部行為進行變更。

- `nil` 帳戶將不再被視為 `LocalDrive/LocalStorage` 位置的目前帳戶。傳入 `nil` 帳戶會將它視為 `Unmanaged` 帳戶。因為應用程式可以控制其處理沙箱儲存體的方式, 所以身分識別可以而且應該與這些位置相關聯。
- 帳戶將不再被視為單一 `nil` 身分識別應用程式的目前帳戶。現在, 在單一 `nil` 身分識別應用程式中傳入帳戶的處理方式會與傳遞至多重身分識別應用程式時完全相同。如果您正在開發單一身分識別應用程式, 請使用 `IntuneMAMPolicy` 的 `primaryUser` 在受控 `nil` 時參考目前的帳戶, 並在未受管理時參考目前的帳戶。

處理儲存至案例

將資料移至新的雲端儲存體或本機位置之前, 應用程式必須先向 `isSaveToAllowedForLocation:withAccount:` API 確認 IT 系統管理員是否允許資料傳輸。這個方法會在 物件上 `IntuneMAMPolicy` 呼叫。要就地編輯和儲存的資料不需要使用此 API 來檢查。

NOTE

物件 `IntuneMAMPolicy` 應該代表所儲存資料擁有者的原則。若要取得 `IntuneMAMPolicy` 特定身分識別的物件，請呼叫 `IntuneMAMPolicyManager` 的 `policyForIdentity:` 方法。如果擁有者是沒有身分識別的 Unmanaged 帳戶，`nil` 則可以傳遞至 `policyForIdentity:`。即使要儲存的資料不是組織資料，`isSaveToAllowedForLocation:withAccount:` 仍應呼叫。擁有目的地位置的帳戶可能仍有限制傳入 Unmanaged 資料的原則。

方法 `isSaveToAllowedForLocation:withAccount:` 接受兩個引數。第一個引數是中 `IntuneMAMPolicy.h` 定義之型 `IntuneMAMSaveLocation` 別的列舉值。第二個引數是擁有位置之身分識別的 UPN。如果不知道擁有者，`nil` 則可以改用。

支援的儲存位置

Intune MAM SDK 支援中 `IntuneMAMPolicy.h` 定義的下列儲存位置：

- `IntuneMAMSaveLocationOneDriveForBusiness` - 此位置代表商務用 OneDrive 位置。與 OneDrive 帳戶相關聯的身分識別應該作為第二個引數傳入。
- `IntuneMAMSaveLocationSharePoint` - 此位置同時代表 SharePoint Online 和 AAD Hybrid Modern Auth SharePoint 內部部署位置。與 SharePoint 帳戶相關聯的身分識別應該作為第二個引數傳入。
- `IntuneMAMSaveLocationLocalDrive` - 此位置代表只能由應用程式存取的應用程式沙箱儲存體。此位置 **不應** 用於透過檔案選擇器儲存，或透過共用擴充功能儲存至檔案。如果身分識別可以與 app-sandbox 儲存體相關聯，則應該將它當做第二個引數傳入。如果沒有身分識別，`nil` 則應該改為傳遞。(例如，應用程式可能會針對不同的帳戶使用個別的應用程式沙箱儲存體容器。在此情況下，擁有所存取容器的帳戶應該作為第二個引數。)
- `IntuneMAMSaveLocationCameraRoll` - 此位置代表 iOS 相片庫。因為沒有與 iOS 相片庫相關聯的帳戶，所以只有在使用此位置時，才 `nil` 應該傳遞為第二個引數。
- `IntuneMAMSaveLocationAccountDocument` - 此位置代表先前未列出可系結至受管理帳戶的任何組織位置。與位置相關聯的組織帳戶應該作為第二個引數傳入。(例如，將相片上傳至系結至組織帳戶的組織 LOB 雲端服務。)
- `IntuneMAMSaveLocationOther` - 此位置代表任何非組織、先前未列出或任何未知的位置。如果帳戶與位置相關聯，則應該將它當做第二個引數傳入。否則，`nil` 應該改用。

儲存位置的特殊考慮

位置 `IntuneMAMSaveLocationLocalDrive` 應該只用於只能由應用程式存取的 app-sandbox 儲存體。若要檢查檔案是否可以透過檔案選擇器儲存至 iOS 裝置儲存體，或使用檔案應用程式 `IntuneMAMSaveLocationOther` 中可存取資料的其他方法。

如果未列出目的地位置，`IntuneMAMSaveLocationAccountDocument` 則應該使用或 `IntuneMAMSaveLocationOther`。

如果位置包含使用受管理帳戶存取的組織資料，(即。應使用 LOB 雲端服務來儲存組織資料)

`IntuneMAMSaveLocationAccountDocument`。如果位置不包含組織資料，則 `IntuneMAMSaveLocationOther` 應該使用位置。

處理開放式案例

從新的雲端儲存體或本機位置匯入資料之前，應用程式必須先向 `isOpenFromAllowedForLocation:withAccount:` API 檢查，以瞭解 IT 系統管理員是否允許資料傳輸。這個方法會在物件上 `IntuneMAMPolicy` 呼叫。就地開啟的資料不需要使用此 API 進行檢查。

NOTE

物件 `IntuneMAMPolicy` 應該代表接收資料之身分識別的原則。若要取得 `IntuneMAMPolicy` 特定身分識別的物件，請呼叫 `IntuneMAMPolicyManager` 的 `policyForIdentity:` 方法。如果接收帳戶是沒有身分識別的 Unmanaged 帳戶，`nil` 則可以傳遞至 `policyForIdentity:`。即使收到的資料不是組織資料，`isOpenFromAllowedForLocation:withAccount:` 仍應呼叫。擁有資料的帳戶可能仍有限制傳出資料傳輸目的地的原則。

方法 `isOpenFromAllowedForLocation:withAccount:` 接受兩個引數。第一個引數是中 `IntuneMAMPolicy.h` 定義之型 `IntuneMAMOpenLocation` 別的列舉值。第二個引數是擁有位置之身分識別的 UPN。如果不知道擁有者, `nil` 則可以改用。

支援的開啟位置

Intune MAM SDK 支援中 `IntuneMAMPolicy.h` 定義的下列開放位置：

- `IntuneMAMOpenLocationOneDriveForBusiness` - 此位置代表商務用 OneDrive 位置。與 OneDrive 帳戶相關聯的身分識別應該作為第二個引數傳入。
- `IntuneMAMOpenLocationSharePoint` - 此位置同時代表 SharePoint Online 和 AAD Hybrid Modern Auth SharePoint 內部部署位置。與 SharePoint 帳戶相關聯的身分識別應該作為第二個引數傳入。
- `IntuneMAMOpenLocationCamera` - 此位置 僅 代表相機所拍攝的新影像。因為沒有與 iOS 相機相關聯的帳戶, 所以只有在使用此位置時, 才 `nil` 應該傳遞作為第二個引數。若要從 iOS 相片庫開啟資料, 請使用 `IntuneMAMOpenLocationPhotos`。
- `IntuneMAMOpenLocationPhotos` - 此位置 僅 代表 iOS 相片庫內的現有影像。因為沒有與 iOS 相片庫相關聯的帳戶, 所以只有在使用此位置時, 才 `nil` 應該傳遞為第二個引數。若要開啟直接從 iOS 相機擷取的影像, 請使用 `IntuneMAMOpenLocationCamera`。
- `IntuneMAMOpenLocationLocalStorage` - 此位置代表只能由應用程式存取的應用程式沙箱儲存體。此位置 不應 用於從檔案選擇器開啟檔案, 或處理來自 openURL 的傳入檔案。如果身分識別可以與 app-sandbox 儲存體相關聯, 則應該將它當做第二個引數傳入。如果沒有身分識別, `nil` 則應該改為傳遞。(例如, 應用程式可能會針對不同的帳戶使用個別的應用程式沙箱儲存體容器。在此情況下, 擁有所存取容器的帳戶應該作為第二個引數。)
- `IntuneMAMOpenLocationAccountDocument` - 此位置代表先前未列出可系結至受管理帳戶的任何組織位置。與位置相關聯的組織帳戶應該作為第二個引數傳入。(例如, 從組織與組織帳戶系結的 LOB 雲端服務下載相片。)
- `IntuneMAMOpenLocationOther` - 此位置代表任何非組織位置、先前未列出的位置, 或任何未知的位置。如果帳戶與位置相關聯, 則應該將它當做第二個引數傳入。否則, `nil` 應該改用。

開放位置的特殊考慮

位置 `IntuneMAMOpenLocationLocalStorage` 應該只用於應用程式可存取的應用程式沙箱儲存體。若要檢查是否可以透過檔案選擇器或檔案應用程式中也可存取資料的其他方法, 從 iOS 裝置儲存體開啟檔案, `IntuneMAMOpenLocationOther` 請使用。

如果未列出目的地位置, `IntuneMAMOpenLocationAccountDocument` 則應該使用 或 `IntuneMAMOpenLocationOther`。如果位置包含使用受管理帳戶存取的組織資料, (即。應使用 LOB 雲端服務來儲存組織資料) `IntuneMAMOpenLocationAccountDocument`。如果位置不包含組織資料, 則 `IntuneMAMSaveLocationOther` 應該使用位置。

處理傳入的 NSItemProviders 和檔案

若要處理從共用延伸模組接收的 NSItemProviders, `IntuneMAMPolicy` 可以使用的 `canReceiveSharedItemProvider:` 方法, 而不是 `isOpenFromAllowedForLocation:withAccount:`。方法 `canReceiveSharedItemProvider:` 會採用 NSItemProvider, 並傳回 IT 系統管理員是否允許它開啟至 `IntuneMAMPolicy` 物件的帳戶。在呼叫此方法之前, 必須先載入專案 (例如呼叫 `loadItemForTypeIdentifier:options:completionHandler`)。您也可以從傳遞至 NSItemProvider 載入呼叫的完成處理常式呼叫這個方法。

若要處理傳入檔案, `IntuneMAMPolicy` 可以使用的 `canReceiveSharedFile:` 方法, 而不是 `isOpenFromAllowedForLocation:withAccount:`。方法 `canReceiveSharedFile:` 會採用 NSString 路徑, 並傳回 IT 系統管理員是否允許它開啟至 `IntuneMAMPolicy` 物件的帳戶。

共用封鎖的警示

呼叫 或 `isOpenFromAllowedForLocation:withAccount:` API 並找到 封鎖儲存/開啟動作時, `isSaveToAllowedForLocation:withAccount:` 可以使用 UI 協助程式函式。如果應用程式想要通知使用者已封鎖動作, 它可以呼叫 `showSharingBlockedMessage` 中 `IntuneMAMUIHelper.h` 定義的 API, 以顯示具有一般訊息的警示檢視。

透過 UIActivityViewController 共用資料

從 8.0.2 版開始，Intune App SDK 可以篩選 `UIActivityViewController` 動作，讓只有 Intune 受控共用位置可供選取。此行為將由應用程式資料傳輸原則控制。

「複製到」動作

透過 `UIActivityViewController` 和 `UIDocumentInteractionController` 共用檔時，iOS 會針對支援開啟所共用檔的每個應用程式顯示「複製到」動作。應用程式會透過其 Info.plist 中的設定來宣告其支援 `CFBundleDocumentTypes` 的檔案類型。如果原則禁止共用至 Unmanaged 應用程式，將無法再使用這種共用類型。作為取代，使用者必須將非 UI 動作延伸模組新增至其應用程式，並將其連結至 Intune App SDK。動作延伸模組只是存根。SDK 會實作檔案共用行為。請遵循下列步驟：

1. 您的應用程式必須在其 Info.plist `CFBundleURLTypes` 下定義至少一個 schemeURL 及其對應專案

`-intunemam`。例如：

```
<key>CFBundleURLSchemes</key>
<array>
  <string>launch-com.contoso.myapp</string>
  <string>launch-com.contoso.myapp-intunemam</string>
</array>
```

2. 您的應用程式和動作延伸模組必須至少共用一個應用程式群組，而且應用程式群組必須列在應用程式的和延伸模組的 IntuneMAMSettings 字典底下的陣列底下 `AppGroupIdentifiers`。
3. 您的應用程式和動作延伸模組都必須具有 Keychain 共用功能，並共用 `com.microsoft.intune.mam` 金鑰鏈群組。
4. 將動作延伸模組命名為「Open in」，後面接著應用程式名稱。視需要將 Info.plist 當地語系化。
5. 提供延伸模組的範本圖示，如 [Apple 開發人員檔](#) 所述。或者，IntuneMAMConfigurator 工具可用來從應用程式 .app 目錄產生這些映射。若要執行這項作業，請執行：

```
IntuneMAMConfigurator -generateOpenInIcons /path/to/app.app -o /path/to/output/directory
```

6. 在延伸模組 Info.plist 的 IntuneMAMSettings 底下，新增名為且值為 `OpenInActionExtension` YES 的布林值設定。
7. 將設定 `NSExtensionActivationRule` 為支援單一檔案，以及應用程式 `CFBundleDocumentTypes` 前置 `com.microsoft.intune.mam` 詞為的所有類型。例如，如果應用程式支援 public.text 和 public.image，則啟用規則會是：

```
SUBQUERY (
  extensionItems,
  $extensionItem,
  SUBQUERY (
    $extensionItem.attachments,
    $attachment,
    ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO
    "com.microsoft.intune.mam.public.text" ||
    ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO
    "com.microsoft.intune.mam.public.image").@count == 1
  ).@count == 1
```

更新現有的共用和動作延伸模組

如果您的應用程式已經包含共用或動作延伸模組，則必須修改它們 `NSExtensionActivationRule` 才能允許 Intune 類型。針對擴充功能所支援的每個類型，新增前面加上 `com.microsoft.intune.mam` 的其他類型。例如，如果現有

的啟用規則：

```
SUBQUERY (
    extensionItems,
    $extensionItem,
    SUBQUERY (
        $extensionItem.attachments,
        $attachment,
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "public.url" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "public.plain-text" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "public.image" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "public.data"
    ).@count > 0
).@count > 0
```

它應該變更為：

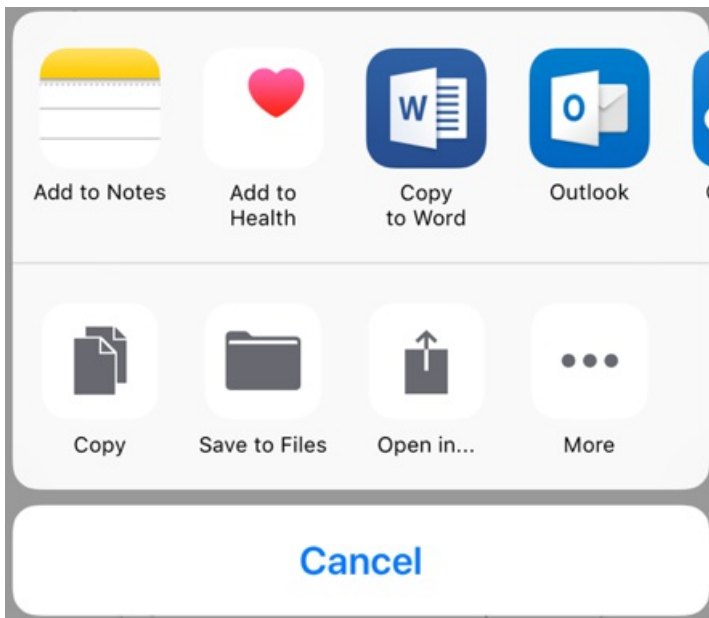
```
SUBQUERY (
    extensionItems,
    $extensionItem,
    SUBQUERY (
        $extensionItem.attachments,
        $attachment,
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "public.url" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "public.plain-text" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "public.image" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "public.data" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "com.microsoft.intune.mam.public.url" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "com.microsoft.intune.mam.public.plain-
text" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "com.microsoft.intune.mam.public.image" ||
        ANY $attachment.registeredTypeIdentifiers UTI-CONFORMS-TO "com.microsoft.intune.mam.public.data"
    ).@count > 0
).@count > 0
```

NOTE

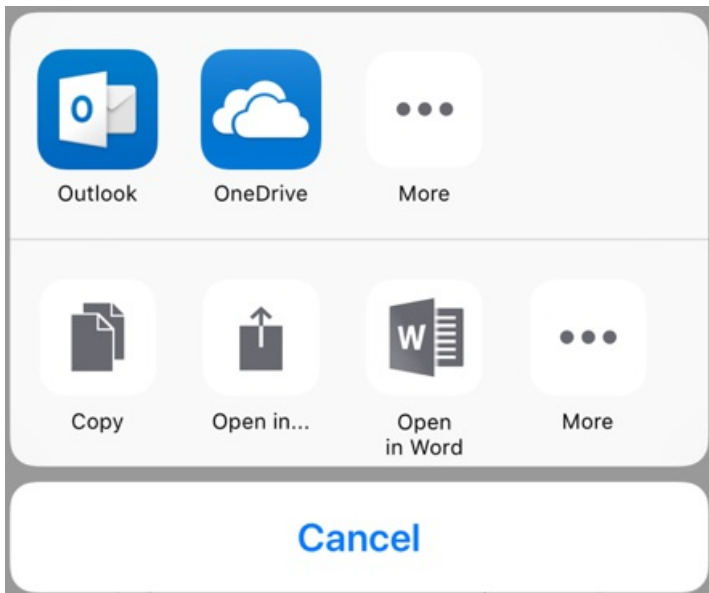
IntuneMAMConfigurator 工具可用來將Intune類型新增至啟用規則。如果您現有的啟用規則使用預先定義的字串常數 (例如 `NSExtensionActivationSupportsFileWithMaxCount`、`NSExtensionActivationSupportsText` 等)，則述詞語法可能會變得相當複雜。IntuneMAMConfigurator 工具也可用來將啟用規則從字串常數轉換成述詞字串，同時新增Intune類型。

UI 看起來應該像什麼

舊的 UI：



新的 UI:



為您的 iOS 應用程式啟用目標設定 (APP/MAM 應用程式設定)

MAM 目標設定 (也稱為 MAM 應用程式設定) 可讓應用程式透過 Intune SDK 接收設定資料。此資料的格式和變體必須由應用程式擁有者/開發人員定義並傳達給 Intune 客戶。

Intune 系統管理員可以透過 [Microsoft 端點管理員](#) 系統管理中心和 Intune 圖形 API 來鎖定及部署設定資料。從 7.0.1 版的 Intune App SDK for iOS 開始，參與 MAM 目標設定的應用程式可以透過 MAM 服務提供 MAM 目標設定資料。應用程式設定資料會透過 MAM 服務直接推送至應用程式，而不是透過 MDM 通道。Intune App SDK 提供類別來存取從這些主控台擷取的資料。下列專案是必要條件：

- 您必須先向 Intune MAM 服務註冊應用程式，才能存取 MAM 目標設定 UI。如需詳細資訊，請 [參閱接收應用程式保護原則](#)。
- 包含 `IntuneMAMAppConfigManager.h` 在應用程式的原始程式檔中。
- 呼叫 `[[IntuneMAMAppConfigManager instance] appConfigForIdentity:]` 以取得應用程式組態物件。
- 在物件上 `IntuneMAMAppConfig` 呼叫適當的選取器。例如，如果您應用程式的金鑰是字串，您會想要使用 `stringValueForKey` 或 `allStringsForKey`。如需傳回值和錯誤狀況的詳細描述，請參閱 `IntuneMAMAppConfig.h`。

如需圖形 API 功能的詳細資訊，請參閱圖形 API 參考。

如需如何在 iOS 中建立 MAM 目標應用程式設定原則的詳細資訊，請參閱[如何使用 iOS/iPadOS 的 Microsoft Intune 應用程式設定原則](#)中的 MAM 目標應用程式設定一節。

應用程式保護 CA 支援 (選擇性)

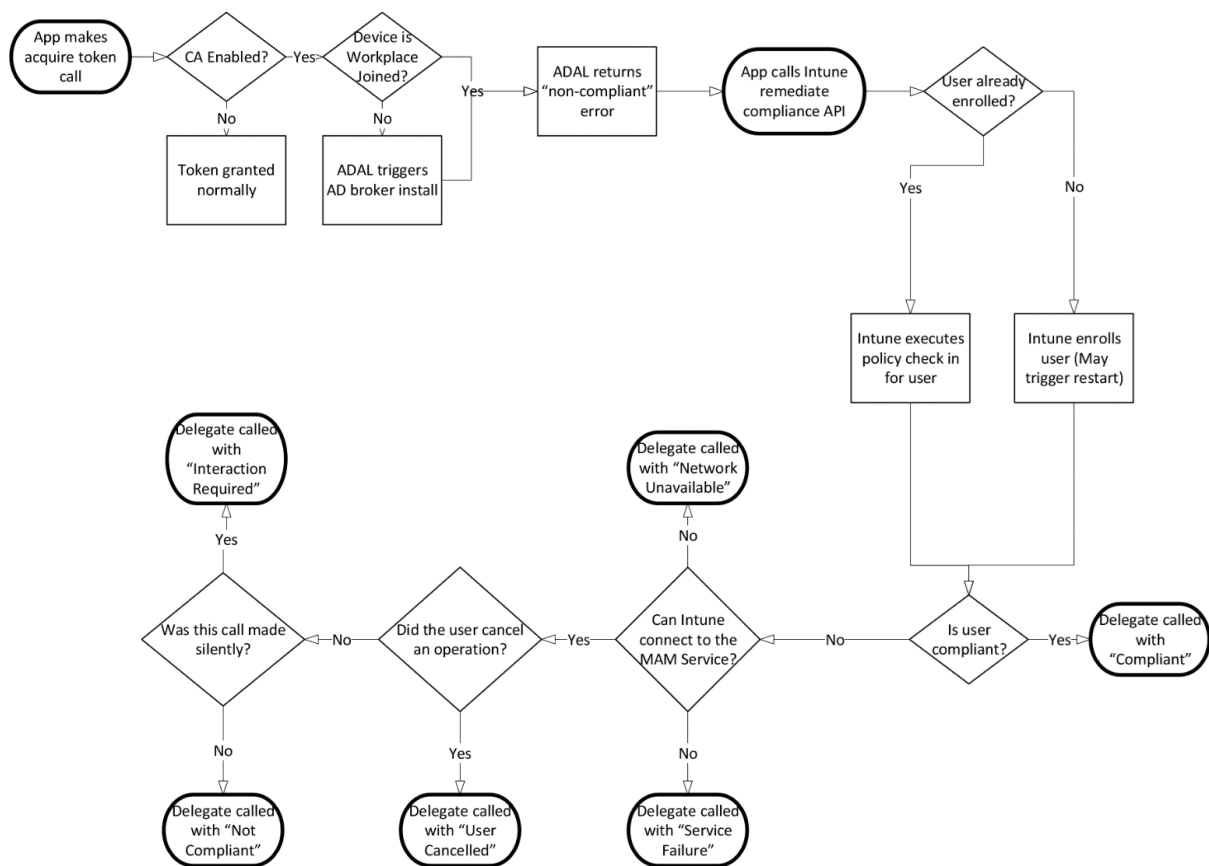
應用程式保護條件式存取會封鎖對伺服器權杖的存取，直到 Intune 確認已套用應用程式保護原則為止。這項功能需要變更您新增的使用者流程。一旦客戶啟用應用程式保護 CA，該客戶租使用者中存取受保護資源的應用程式將無法取得存取權杖，除非他們支援這項功能。

相依性

除了 Intune SDK，您還需要這兩個元件，才能在您的應用程式中啟用應用程式保護 CA。

1. iOS 驗證器應用程式
2. MSAL 驗證程式庫 1.0 或更新版本

MAM-CA 補救流程



新的 API

大部分的新 API 都可以在 IntuneMAMComplianceManager.h 中找到。應用程式必須留意下列三種行為差異。

❖	❖
應用程式 → ADAL/MSAL：取得權杖	當應用程式嘗試取得權杖時，應該準備好接收 ERROR_SERVER_PROTECTION_POLICY_REQUIRED。應用程式在其初始帳戶新增流程期間或稍後在應用程式生命週期中存取權杖時，可能會收到此錯誤。當應用程式收到此錯誤時，將不會被授與存取權杖，而且需要修復才能擷取任何伺服器資料。

III	II
應用程式 → Intune SDK: 呼叫 <code>remediateComplianceForIdentity</code>	當應用程式收到來自 ADAL 的 <code>ERROR_SERVER_PROTECTION_POLICY_REQUIRED</code> 或 <code>MSALErrorServerProtectionPoliciesRequired</code> 時, 應該呼叫 <code>[[IntuneMAMComplianceManager 實例] remediateComplianceForIdentity]</code>, 讓 Intune 註冊應用程式並套用原則。此呼叫期間可能會重新開機應用程式。如果應用程式需要在重新開機之前儲存狀態, 它可以在 <code>IntuneMAMPolicyDelegate</code> 的 <code>restartApplication</code> 委派方法中儲存狀態。 <code>remediateComplianceForIdentity</code> 提供 <code>registerAndEnrollAccount</code> 和 <code>loginAndEnrollAccount</code> 的所有功能。因此, 應用程式不需要使用這其中一個較舊的 API。
Intune → 應用程式: 委派補救通知	Intune 擷取並套用原則之後, 它會使用 <code>IntuneMAMComplianceDelegate</code> 通訊協定通知應用程式結果。如需應用程式應如何處理每個錯誤的資訊, 請參閱 <code>IntuneComplianceManager.h</code> 中的 <code>IntuneMAMComplianceStatus</code>。在 <code>IntuneMAMComplianceComplianceCompliant</code> 以外的所有情況下, 使用者都不會有有效的存取權杖。 如果應用程式已經有受控內容, 而且無法進入符合規範的狀態, 應用程式應該呼叫選擇性抹除來移除任何公司內容。 如果我們無法達到符合規範的狀態, 應用程式應該會顯示由 <code>ErrorMessage</code> 和 <code>andErrorTitle</code> 提供的當地語系化錯誤訊息和標題字串。

IntuneMAMComplianceDelegate 的 `hasComplianceStatus` 方法範例

```

(void) identity:(NSString*) identity hasComplianceStatus:(IntuneMAMComplianceStatus) status withErrorString:
(NSString*) error;
{
    switch(status)
    {
        case IntuneMAMComplianceCompliant:
        {
            /*
             Handle successful compliance
            */
            break;
        }
        case IntuneMAMComplianceNotCompliant:
        case IntuneMAMComplianceNetworkFailure:
        case IntuneMAMComplianceUserCancelled:
        case IntuneMAMComplianceServiceFailure:
        {
            UIAlertController* alert = [UIAlertController alertControllerWithTitle:identity
            message:error
            preferredStyle:UIAlertControllerStyleAlert];
            UIAlertAction* defaultAction = [UIAlertAction actionWithTitle:@"OK"
            style:UIAlertActionStyleDefault
            handler:^(UIAlertAction * action) {exit(0);}];
            [alert addAction:defaultAction];
            dispatch_async(dispatch_get_main_queue(), ^{
            [self presentViewController:alert animated:YES completion:nil];
            });
            break;
        }
        case IntuneMAMComplianceInteractionRequired:
        {
            [[IntuneMAMComplianceManager instance] remediateComplianceForIdentity:identity silent:NO];
            break;
        }
    }
}
}

```

```

func identity(_ identity: String, hasComplianceStatus status: IntuneMAMComplianceStatus, withErrorMessage
errMsg: String, andErrorTitle errTitle: String) {
    switch status {
        case .compliant:
            //Handle successful compliance
        case .notCompliant, .networkFailure, .serviceFailure, .userCancelled:
            DispatchQueue.main.async {
                let alert = UIAlertController(title: errTitle, message: errMsg, preferredStyle: .alert)
                alert.addAction(UIAlertAction(title: "OK", style: .default, handler: { action in
                    exit(0)
                })))
                self.present(alert, animated: true, completion: nil)
            }
        case .interactionRequired:
            IntuneMAMComplianceManager.instance().remediateCompliance(forIdentity: identity, silent: false)
    }
}

```

MSAL/ADAL

應用程式必須將用戶端功能變數新增至其 MSAL/ADAL 組態，以指出應用程式保護 CA 的支援。需要下列值：宣告 = {「access_token」:{「xms_cc」:{「values」:[「protapp」]}}}

[MSALPublicClientApplicationConfig 類別參考 \(azuread.github.io\)](#)

```

MSALAADAuthority *authority = [[MSALAADAuthority alloc] initWithURL:[NSURL alloc]
initWithString:IntuneMAMSettings.aadAuthorityUriOverride error:&msalError];
MSALPublicClientApplicationConfig *config = [[MSALPublicClientApplicationConfig alloc]
initWithClientId:IntuneMAMSettings.aadClientIdOverride
redirectUri:IntuneMAMSettings.aadRedirectUriOverride
authority:authority];

/*
IF YOU'RE IMPLEMENTING CA IN YOUR APP, PLEASE PAY ATTENTION TO THE FOLLOWING...
*/
// This is needed for CA!
// This line adds an option to the MSAL token request so that MSAL knows that CA may be active
// Without this, MSAL won't know that CA could be activated
// In the event that CA is activated and this line isn't in place, the auth flow will fail

config.clientApplicationCapabilities = @[@"protapp"];

```

```

guard let authorityURL = URL(string: kAuthority) else {
    print("Unable to create authority URL")
    return
}
let authority = try MSALAADAuthority(url: authorityURL)
let msalConfiguration = MSALPublicClientApplicationConfig(clientId: kClientID,redirectUri:
kRedirectUri,
                                authority: authority)
msalConfiguration.clientApplicationCapabilities = ["ProtApp"]
self.applicationContext = try MSALPublicClientApplication(configuration: msalConfiguration)

```

如何測試應用程式保護 CA

設定應用程式保護 CA 的測試使用者

1. 使用系統管理員認證登入。<https://portal.azure.com>
2. 選取 [Azure Active Directory > 安全 > 條件式存取 > 新原則]。建立新的條件式存取原則。
3. 設定下列專案以設定條件式存取原則：
 - 填入 [名稱] 字 段。
 - 啟用原則。
 - 將原則指派給使用者或群組。
4. 指派雲端應用程式。選取 [包含 > 所有雲端應用程式]。如警告所示，請小心不要設定此設定錯誤。例如，如果您排除所有雲端應用程式，則會將自己鎖定在主控台外。
5. 選取 [存取控制 > 授與存取權 > 需要應用程式保護原則]，以授與存取控制。
6. 當您完成設定原則時，請選取 [建立] 以儲存原則並加以套用。
7. 啟用原則。
8. 您也必須確定使用者是 MAM 原則的目標。

測試案例

測試案例	預期結果	實際結果
一律套用 MAM-CA	在您的應用程式中註冊之前，請確定使用者同時是應用程式保護 CA 和 MAM 原則的目標。	確認您的應用程式會處理上述補救案例，且應用程式可以取得存取權杖。
在使用者註冊之後套用 MAM-CA	使用者應該已登入應用程式，但不能以應用程式保護 CA 為目標。	在主控台中以應用程式保護 CA 的使用者為目標，並確認您正確地處理 MAM 補救

問題	原因	解決方案
MAM-CA 不符合規範	設定應用程式保護 CA 原則，但不要指派 MAM 原則。	使用者應該無法取得存取權杖。這適用於測試您的應用程式如何處理 IntuneMAMComplianceStatus 錯誤案例。

遙測

根據預設，Intune App SDK for iOS 會收集下列事件種類的遙測：

- **應用程式啟動**：若要協助 Microsoft Intune 瞭解透過 MDM 的管理類型 (MAM、不含 MDM 註冊的 MAM 等)，瞭解已啟用 MAM 的應用程式使用方式。
- **註冊呼叫**：若要協助 Microsoft Intune 瞭解成功率，以及從用戶端起始註冊呼叫的其他效能計量。
- **Intune 動作**：為了協助診斷問題並確保 Intune 功能，我們會收集 SDK 動作 Intune 相關資訊。

NOTE

如果您選擇不要將 Intune App SDK 遙測資料傳送至行動應用程式 Microsoft Intune，則必須停用 Intune 應用程式 SDK 遙測擷取。在 IntuneMAMSettings 字典中，將屬性 `MAMTelemetryDisabled` 設定為 YES。

啟用多重身分識別 (選擇性)

根據預設，SDK 會將原則套用至整個應用程式。多重身分識別是一項 MAM 功能，可讓您在每個身分識別層級上套用原則。相較于其他 MAM 功能，這需要更多應用程式參與。

應用程式必須在想要變更作用中身分識別時通知應用程式 SDK。需要變更身分識別時，SDK 也會通知應用程式。目前僅支援一個受控識別。使用者註冊裝置或應用程式之後，SDK 會使用此身分識別，並將其視為主要受控識別。應用程式中的其他使用者將被視為不受限制的原則設定未受管理。

請注意，身分識別只會定義為字串。身分識別不區分大小寫。針對身分識別對 SDK 的要求可能不會傳回設定身分識別時原先使用的相同大小寫。

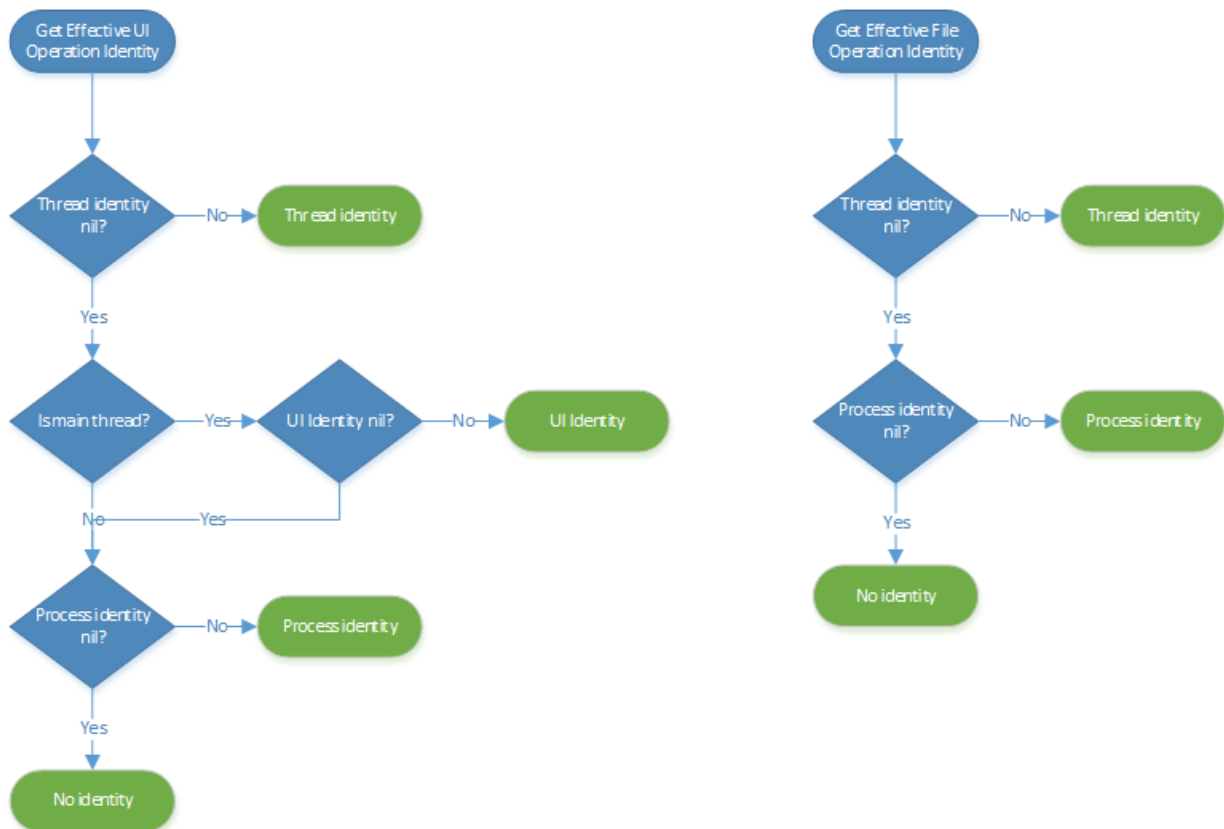
身分識別概觀

身分識別只是帳戶的使用者名稱 (例如，user@contoso.com)。開發人員可以在下列層級設定應用程式的身分識別：

- **進程身分識別**：設定整個進程的身分識別，且主要用於單一身分識別應用程式。此身分識別會影響所有工作、檔案和 UI。
- **UI 身分識別**：決定哪些原則會套用至主執行緒上的 UI 工作，例如剪下/複製/貼上、PIN、驗證和資料共用。UI 身分識別不會影響檔案工作，例如加密和備份。
- **執行緒身分識別**：影響目前線程上套用的原則。此身分識別會影響所有工作、檔案和 UI。

無論使用者是否受到管理，應用程式都須負責適當地設定身分識別。

在任何時候，每個執行緒都有 UI 工作和檔案工作的有效身分識別。這是用來檢查應套用哪些原則的身分識別。如果身分識別為「無身分識別」或使用者未受管理，則不會套用任何原則。下圖顯示如何判斷有效身分識別。



執行緒佇列

應用程式通常會將非同步和同步工作分派給執行緒佇列。SDK 會攔截大中央分派 (GCD) 呼叫，並將目前的執行緒識別與分派的工作產生關聯。當工作完成時，SDK 會暫時將執行緒識別變更為與工作相關聯的身分識別、完成工作，然後還原原始的執行緒識別。

由於 `NSOperationQueue` 是建置在 GCD 之上，`NSOperations` 會在將工作新增至時，于執行緒的身分識別上執行 `NSOperationQueue`。 `NSOperations` 或直接透過 GCD 分派的函式也可以在執行時變更目前的執行緒身分識別。此身分識別會覆寫繼承自分派執行緒的身分識別。

在快速中，由於 SDK 如何傳播的身 `DispatchWorkItem` 分識別，與 `DispatchWorkItem` 相關聯的身分識別是建立專案而非分派該專案之執行緒的執行緒身分識別。

檔案擁有者

SDK 會追蹤本機檔案擁有者的身分識別，並據以套用原則。建立檔案或以截斷模式開啟檔案時，就會建立檔案擁有者。擁有者會設定為執行工作之執行緒的有效檔案工作身分識別。

或者，應用程式可以使用明確地設定檔案擁有者身分識別 `IntuneMAMFilePolicyManager`。應用程式可以使用 `IntuneMAMFilePolicyManager` 來擷取檔案擁有者，並在顯示檔案內容之前設定 UI 身分識別。

共用資料

如果應用程式建立具有 Managed 和 Unmanaged 使用者資料的檔案，則應用程式會負責加密受控使用者的資料。您可以使用 `protect` 中的和 `unprotect` API `IntuneMAMDataProtectionManager` 來加密資料。

方法 `protect` 接受可以是受控或非受控使用者的身分識別。如果使用者受到管理，資料將會加密。如果使用者未受管理，則會將標頭新增至編碼身分識別的資料，但不會加密資料。您可以使用 `protectionInfo` 方法來擷取資料的擁有者。

共用擴充功能

如果應用程式具有共用延伸模組，則可以透過 `protectionInfoForItemProvider` 中的方法 `IntuneMAMDataProtectionManager` 來擷取所共用專案的擁有者。如果共用專案是檔案，SDK 將會處理檔案擁有者的設定。如果共用專案是資料，則應用程式會負責在將此資料保存至檔案時設定檔案擁有者，以及在 UI 中顯示此資料之前呼叫 `setUIPolicyIdentity` API。

開啟多重身分識別

根據預設，應用程式會被視為單一身分識別。SDK 會將進程身分識別設定為已註冊的使用者。若要啟用多重身分識別支援，請將名稱 `MultiIdentity` 和值為 YES 的布林值設定新增至應用程式 Info.plist 檔案中的 `IntuneMAMSettings` 字典。

NOTE

啟用多重身分識別時，進程身分識別、UI 身分識別和執行緒身分識別會設定為 nil。應用程式會負責適當地設定它們。

切換身分識別

● 應用程式起始的身分識別切換：

在啟動時，多重身分識別應用程式會被視為在未知的非受控帳戶下執行。條件式啟動 UI 將不會執行，而且不會在應用程式上強制執行任何原則。應用程式會負責在每次應變更身分識別時通知 SDK。一般而言，每當應用程式即將顯示特定使用者帳戶的資料時，就會發生這種情況。

例如，當使用者嘗試在筆記本中開啟檔、信箱或索引標籤時。應用程式必須先通知 SDK，才能實際開啟檔案、信箱或索引標籤。這是透過中的 `setUIPolicyIdentity` API `IntuneMAMPolicyManager` 來完成。無論使用者是否受管理，都應該呼叫此 API。如果使用者受到管理，SDK 將會執行條件式啟動檢查，例如越獄偵測、PIN 和驗證。

身分識別切換的結果會透過完成處理常式以非同步方式傳回至應用程式。應用程式應該延後開啟檔、信箱或索引標籤，直到傳回成功的結果碼為止。如果身分識別切換失敗，應用程式應該會取消工作。

多重身分識別應用程式應避免使用 `setProcessIdentity` 作為設定身分識別的方式。使用 `UIScenes` 的應用程式應該使用 `setUIPolicyIdentity:forWindow` API 來設定身分識別。

應用程式也可以使用 `setCurrentThreadIdentity:` 和 `setCurrentThreadIdentity:forScope:` 來設定目前線程的身分識別

`setCurrentThreadIdentity:forScope:`。例如，應用程式可能會繁衍背景執行緒、將身分識別設定為受控識別，然後對受控檔案執行檔案作業。如果應用程式使用 `setCurrentThreadIdentity:`，則應用程式也應該使用 `getCurrentThreadIdentity`，以便在完成後還原原始身分識別。不過，如果應用程式使用 `setCurrentThreadIdentity:forScope:`，則會自動還原舊的身分識別。建議使用 `setCurrentThreadIdentity:forScope:`。

由於 `async/await` `[IntuneMAMPolicyManager setCurrentThreadIdentity:]`，且 `[IntuneMAMPolicyManager setCurrentThreadIdentity:forScope:]` 無法使用，因此會快速執行。相反地，在 `swift` 中設定目前的身分識別，請使用 `IntuneMAMSwiftContextManager.setIdentity(_, forScope:)`。此 API 有非同步、擲回和非同步擲回關閉的變體要傳入。

● SDK 起始的身分識別切換：

有時候，SDK 需要要求應用程式切換至特定身分識別。多重身分識別應用程式必須在中

`identitySwitchRequired` 實作方法 `IntuneMAMPolicyDelegate`，以處理此要求。

呼叫這個方法時，如果應用程式可以處理切換至指定身分識別的要求，它應該會傳遞

`IntuneMAMAddIdentityResultSuccess` 至完成處理常式。如果無法處理切換身分識別，應用程式應該會傳 `IntuneMAMAddIdentityResultFailed` 入完成處理常式。

應用程式不需要呼叫 `setUIPolicyIdentity` 來回應此呼叫。如果 SDK 需要應用程式切換至 `Unmanaged` 使用者帳戶，則會將空字串傳遞至 `identitySwitchRequired` 呼叫。

● SDK 起始的身分識別自動註冊：

當 SDK 需要在應用程式中自動註冊使用者以執行動作時，應用程式必須在中

`addIdentity:completionHandler:` `IntuneMAMPolicyDelegate` 實作方法。然後，如果應用程式能夠新增身分識別或 `IntuneMAMAddIdentityResultFailed`，應用程式必須呼叫完成處理常式並傳入

IntuneMAMAddIdentityResultSuccess。

- 選擇性抹除：

選擇性地抹除應用程式時，SDK 會在 中 `IntuneMAMPolicyDelegate` 呼叫 `wipeDataForAccount` 方法。應用程式會負責移除指定的使用者帳戶，以及與其相關聯的任何資料。SDK 能夠移除使用者擁有的所有檔案，而且如果應用程式從 `wipeDataForAccount` 呼叫傳回 FALSE，則會這麼做。

請注意，這個方法是從背景執行緒呼叫。在使用者的所有資料都已移除之前，應用程式不應該傳回值，(如果應用程式傳回 FALSE)，則檔案除外。

Siri 意圖

如果您的應用程式與 Siri 意圖整合，或進行 Siri 意圖的註冊，請務必閱讀 中的 `IntuneMAMPolicy.h` 批 `areSiriIntentsAllowed` 注，以取得支援此案例的指示。

列印

如果您的應用程式實作列印，並在自訂功能表上提供自訂列印動作，請務必使用

`UIPrintInteractionController.isPrintingAvailable()` 來判斷您是否應該將列印動作新增至自訂功能表。

通知

如果您的應用程式收到通知，請務必閱讀 中的 `IntuneMAMPolicy.h` 批 `notificationPolicy` 注，以取得支援此案例的指示。建議應用程式註冊 `IntuneMAMPolicyDidChangeNotification` 中所 `IntuneMAMPolicyManager.h` 述的，並透過金鑰鍵將此值傳達給它們 `UNNotificationServiceExtension`。

Safari Web 延伸模組

如果您的應用程式具有 Safari Web 擴充功能，並支援在擴充功能與父應用程式之間傳送資料，在某些情況下，您的應用程式可能需要支援封鎖資料。若要封鎖資料，請在父應用程式中呼叫 `isAppSharingAllowed` 中的 API

`IntuneMAMPolicy.h`，然後封鎖 Web 擴充功能。

在應用程式內顯示 Web 內容

在 iOS 中，Web 檢視可以用來呈現各種不同的 Web 內容，而不需要離開應用程式的內容。某些應用程式可能也會使用 Web 檢視作為跨多個平臺共用功能和 UI 的方式。

因為 Web 檢視存在於應用程式內，所以會將其公開給潛在的資料外泄。如果使用者能夠流覽至應用程式內的任意外部網頁，(透過刻意的應用程式設計，或是透過轉譯的網頁 html 內容) 中公開的連結進行擷取，則使用者可能能夠從應用程式洩漏受控資料。

Intune MAM SDK 提供數個 API 來處理不同的案例，其中 Managed 和 Unmanaged 內容會透過應用程式內的 Web 檢視呈現。只有當有受控使用者登入應用程式時，才需要呼叫這些 API。請參閱下表，以取得適用於哪一個案例的 API 快速指南。

“	API
只有沒有任意網頁風險的使用者和組織內容	不需要 API
僅限非使用者和非組織內容	在 中設定 <code>TreatAllWebViewsAsUnmanaged``Info.plist</code>

UI	API
使用者/組織和非使用者/非組織內容的混合 (多數非使用者/非組織)	在 中設定 <code>TreatAllWebViewsAsUnmanaged</code> , <code>Info.plist</code> 並在包含使用者或組織資料的 Web 檢視上搭配使用 <code>setWebViewPolicy:forWebViewer:</code> <code>IntuneMAMWebViewPolicyCurrentIdentity</code>
使用者/組織和非使用者/非組織內容的混合 (多數使用者/組織)	僅在 <code>IntuneMAMWebViewPolicyUnmanaged</code> 不包含使用者或組織資料的 Web 檢視上搭配使用 <code>setWebViewPolicy:forWebViewer:</code>
使用者或組織內容, 但有任意網頁的風險	遵循 和 的 <code>TreatAllWebViewsAsUnmanaged</code> <code>setWebViewPolicy:forWebViewer:</code> 適當用法, 也會針對可流覽至任意網頁的 Web 檢視實 <code>IntuneMAMWebViewPolicyDelegate</code> 作。

Web 檢視案例 1: 僅顯示使用者或組織內容的網頁

如果應用程式只使用 Web 檢視作為轉譯使用者或組織內容的方式, 而且網頁檢視巡覽至任意外部網頁沒有風險, 則不需要使用任何 API 或設定。根據預設, SDK 會將應用程式內顯示的任何 Web 檢視視為屬於目前 UI 原則身分識別的內容。

如果受控使用者在應用程式內開啟 Web 檢視, 則任何來自 Web 檢視的剪下/複製資料都會被視為受控內容。貼入 Web 檢視會根據 Managed 帳戶的原則來處理。

如果 Unmanaged 使用者在應用程式內開啟 Web 檢視, 則會將來自 Web 檢視的任何剪下/複製資料視為非受控內容。貼入 Web 檢視會被視為由 Unmanaged 帳戶完成, 而且不會強制執行其他限制。

Web 檢視案例 2: 僅限未顯示使用者或組織內容的網頁

如果應用程式知道永遠不會在 Web 檢視中顯示使用者或組織內容, 則可以在應用程式的 中將 設定為 `TreatAllWebViewsAsUnmanaged` `YES` 。 `Info.plist` 這會將網頁檢視中任何使用者完成的所有剪下、複製和貼上動作視為非受控。不論用來執行動作之帳戶的管理狀態為何, 動作都會被視為非受控使用者所執行。

這麼做可確保 Managed 應用程式內容不會透過 Web 檢視洩漏到應用程式外部。如果應用程式只使用 Web 檢視來顯示隱私權注意事項、EULA 或其他不需要使用者檢視的靜態頁面內容, 則設定此旗標會是不錯的主意。

設定時 `TreatAllWebViewsAsUnmanaged` , 網頁檢視內顯示的所有內容 都可以 複製並貼到其他非受控應用程式, 因為 Web 檢視本身會被視為非受控。

Web 檢視案例 3: 混合使用者/組織和非使用者/非組織內容

更複雜的應用程式可能會使用使用者/組織和非使用者/非組織 Web 檢視的組合。應用程式可能會使用 Web 檢視來顯示隱私權注意事項, 但也使用 Web 檢視來呈現使用者內容。在此情況下, `IntuneMAMPolicyManager` 可以使用的 `setWebViewPolicy:forWebViewer:` API。此 API 可讓應用程式將個別 Web 檢視標示為 Unmanaged, 或復原個別 Web 檢視的 `TreatAllWebViewsAsUnmanaged` 效果。

API 接受兩個引數。第一個值是 類型的列舉值 `IntuneMAMWebViewPolicy` 。第二個可以是可能在其子檢視階層中包含 WKWebView 的 UIView 或 UIViewController。WKWebView 本身也可以直接作為第二個引數傳入。

如果 WKWebView 是傳入做為第二個引數的 UIView 或 UIViewController 子系, 則在呼叫此 API 時, 它不需要存在於檢視階層內。在 UIView 或 UIViewController 中傳遞的任何子系 WKWebViews 在新增時, 都會套用適當的原則。

- `IntuneMAMWebViewPolicyUnset` - 這是所有 WKWebViews 的預設原則。Web 檢視只會根據 旗標來處理。
- `IntuneMAMWebViewPolicyUnmanaged` - 使用者在以此原則標記的 Web 檢視上執行的任何剪下/複製/貼上動作,

都會被視為由 Unmanaged 身分識別執行。此原則會覆寫 旗標 `TreatAllWebViewsAsUnmanaged`。

- `IntuneMAMWebViewPolicyCurrentIdentity` - 使用者在以此原則標記的 Web 檢視上執行的任何剪下/複製/貼上動作，將會被視為目前 UI 原則識別所執行的動作。此原則會覆寫 旗標 `TreatAllWebViewsAsUnmanaged`。

大部分的非使用者和非組織資料

如果應用程式內大部分的 Web 檢視都顯示 Unmanaged 內容，則 `TreatAllWebViewsAsUnmanaged` 可以在應用程式的 `Info.plist` 中設定，並 `setWebViewPolicy:forWebView:` `IntuneMAMWebViewPolicyCurrentIdentity` 使用 在使用者或組織內容 Web 檢視上呼叫。

多數使用者和組織資料

如果應用程式內大部分的 Web 檢視顯示使用者或組織內容，則只需要 `setWebViewPolicy:forWebView:` `IntuneMAMWebViewPolicyUnmanaged` 在 Unmanaged Web 檢視上呼叫，因為所有 Web 檢視預設都會被視為受管理。

Web 檢視案例 4: 使用者或組織內容，但有任意網頁的風險

如果網頁檢視是用來顯示使用者或組織內容，但有流覽至任意外部 URL 的風險，則可以搭配

`TreatAllWebViewsAsUnmanaged` `setWebViewPolicy:forWebView:` 和使用額外的 API。例如，建議具有搜尋引擎直接或間接連結的功能或意見反應網頁。

`IntuneMAMWebViewPolicyDelegate` 可以使用 `IntuneMAMPolicyManager` `setWebViewPolicyDelegate:forWebView:` 的實作並設定為 Web 檢視。`IntuneMAMWebViewPolicyDelegate` 有一個必要方法。`isExternalURL:`

方法 `setWebViewPolicyDelegate:forWebView:` 必須直接在 `WKWebView` 或 `SFSafariViewController` 上呼叫。

每次網頁檢視流覽至新頁面時，`isExternalURL:` 都會呼叫委派方法。應用程式應該判斷傳遞至委派方法的 URL 是否代表可以貼入使用者或組織資料的內部網站，或是可能洩漏組織資料的外部網站。傳回 `NO` 會告訴 SDK 正在載入的網站是可共用使用者或組織資料的組織位置。如果目前的原則設定需要，傳回 `YES` 會造成 SDK 在受管理的瀏覽器中開啟 URL，而不是 `WKWebView` 或 `SFSafariViewController`。這可確保應用程式內的任何使用者或組織資料都無法外泄至外部網站。

Web 檢視 API 範例

應用程式建置了五個 Web 檢視 (A、B、C、D 和 E)。Web 檢視 A、B 和 C 不會顯示使用者或組織資料。Web 檢視 D 會顯示可供公司所有使用者使用的組織頁面。Web 檢視 E 會轉譯可能包含連結的使用者檔。

由於大部分的 Web 檢視都是非受控 (A、B 和 C)，因此我們可以將設定 `TreatAllWebViewsAsUnmanaged` 為減少需要呼叫 `setWebViewPolicy:forWebView:` 的次數。

由於 Web 檢視 D 和 E 會顯示使用者內容，且所有 Web 檢視現在預設為非受控，因此我們需要使用

`IntuneMAMWebViewPolicyCurrentIdentity` 標記它們 `setWebViewPolicy:forWebView:`。

因為 Web 檢視 E 包含使用者可能會按一下的連結，而且可用來巡覽至任意 URL，所以我們也需要

`IntuneMAMWebViewPolicyDelegate` 實作，並使用 `setWebViewPolicyDelegate:forWebView:` 將它設定為 Web 檢視 E。在我們的 `isExternalURL:` 實作中，我們可以檢查連入 URL，並查看它們是否與檔的 URL 相同。如果它們不相符，則我們知道它是外部 URL，而且可以傳回 `YES`。如果它們相符，則我們知道它是內部 URL，而且可以傳回 `NO`。

實作和呼叫這些 API 表示受控使用者或組織內容無法洩漏至 Web 檢視 A、B 和 C。這也表示受控內容無法透過按一下檔內的連結，洩漏至使用者可能在 E 中流覽的任何外部 URL。受控內容也會受到保護，方法是防止來自 Web 檢視 D 和 E 的資料洩漏到應用程式外部。

SwiftUI 支援

新建立的 SwiftUI 應用程式支援 `UIScenes`，但預設不會實作 `UISceneDelegate`。如果您的應用程式想要支援 `UIScenes` 並使用 Intune App SDK，則必須實作 `UISceneDelegate`。如果不想支援 `UIScenes`，

`UIApplicationSceneManifest` 則必須移除應用程式 `Info.plist` 中也命名為「應用程式場景資訊清單」設定的 (。

iOS 最佳做法

以下是針對 iOS 開發的建議最佳做法：

- iOS 檔案系統會區分大小寫。請確定這類檔案名 `IntuneMAMResources.bundle` 的案例正確無誤。

常見問題集

所有 API 是否可透過原生 Swift 或 Objective-C 和 Swift 互通性來定址？

Intune 應用程式 SDK API 僅限 Objective-C，不支援原生 Swift。需要 Swift 與 Objective-C 的互通性。

應用程式的所有使用者是否都需要向 APP-WE 服務註冊？

否。事實上，只有公司或學校帳戶應該向 Intune App SDK 註冊。應用程式負責判斷帳戶是否用於工作或學校內容中。

已經登入應用程式的使用者呢？是否需要註冊？

應用程式負責在成功驗證使用者之後註冊使用者。應用程式也負責註冊應用程式具有無 MDM MAM 功能之前可能已存在的任何現有帳戶。

若要這樣做，應用程式應該使用 `registeredAccounts:` 方法。這個方法會傳回 `NSDictionary`，該 `NSDictionary` 已將所有帳戶註冊到 Intune MAM 服務。如果應用程式中的任何現有帳戶不在清單中，應用程式應該透過

`registerAndEnrollAccount:` 註冊這些帳戶。

SDK 重試註冊的頻率為何？

SDK 會在 24 小時間隔內自動重試所有先前失敗的註冊。SDK 會這麼做，以確保如果使用者的組織在使用者登入應用程式之後啟用 MAM，使用者將會成功註冊和接收原則。

SDK 會在偵測到使用者已成功註冊應用程式時停止重試。這是因為只有一位使用者可以在特定時間註冊應用程式。如果使用者未註冊，重試會在相同的 24 小時間隔中重新開始。

為什麼需要取消註冊使用者？

SDK 會定期在背景中採取下列動作：

- 如果應用程式尚未註冊，它會每隔 24 小時嘗試註冊所有已註冊的帳戶。
- 如果應用程式已註冊，SDK 會每隔 8 小時檢查一次 MAM 原則更新。

取消註冊使用者會通知 SDK 使用者將不再使用應用程式，而且 SDK 可以停止該使用者帳戶的任何定期事件。它也會在必要時觸發應用程式取消註冊和選擇性抹除。

我是否應該在 `deregister` 方法中將 `doWipe` 旗標設定為 `true`？

在使用者登出應用程式之前，應該先呼叫這個方法。如果使用者的資料在登出過程中從應用程式中刪除，

`doWipe` 可以設定為 `false`。但是，如果應用程式未移除使用者的資料，`doWipe` 應該設定為 `true`，讓 SDK 可以刪除資料。

是否有任何其他方法可以取消註冊應用程式？

是，IT 系統管理員可以將選擇性抹除命令傳送至應用程式。這會取消註冊和取消註冊使用者，而且會抹除使用者的資料。SDK 會自動處理此案例，並透過取消註冊委派方法傳送通知。

是否有示範如何整合 SDK 的範例應用程式？

是！請參閱 [Chatr 範例應用程式](#)。

如何對我的應用程式進行疑難排解？

Intune SDK for iOS 9.0.3+ 支援在行動應用程式內新增診斷主控台以測試原則和記錄錯誤的能力。

`IntuneMAMDiagnosticConsole.h`IntuneMAMDiagnosticConsole` 定義類別介面，開發人員可用來顯示診斷主控台

Intune。這可讓終端使用者或開發人員在測試期間收集和共用 Intune 記錄，以協助診斷他們可能遇到的任何問題。此 API 對整合者而言是選擇性的。

將您的應用程式提交至App Store

Intune App SDK 的靜態程式庫和架構組建都是通用二進位檔。這表示它們具有所有裝置和模擬器架構的程式碼。如果應用程式有模擬器程式碼，Apple 將會拒絕提交至App Store。針對僅限裝置組建的靜態程式庫進行編譯時，連結器會自動去除模擬器程式碼。請遵循下列步驟，以確保在您將應用程式上傳至App Store之前，已移除所有模擬器程式碼：

1. 請確定 `IntuneMAM.framework` 位於您的桌面上。

2. 執行下列命令：

```
lipo ~/Desktop/IntuneMAM.framework/IntuneMAM -remove i386 -remove x86_64 -output  
~/Desktop/IntuneMAM.device_only
```

```
cp ~/Desktop/IntuneMAM.device_only ~/Desktop/IntuneMAM.framework/IntuneMAM
```

第一個命令會從架構的 DYLIB 檔案中刪除模擬器架構。第二個命令會將僅限裝置的 DYLIB 檔案複製回架構目錄。

使用 Intune App Wrapping Tool 準備應用程式保護原則的 Android 應用程式

2022/9/27 •

使用適用於 android 的 Microsoft Intune App Wrapping Tool，透過限制應用程式的功能來變更內部 Android 應用程式的行為，而不會變更應用程式的程式碼。

工具是在 PowerShell 中執行的 Windows 命令列應用程式，並在您的 Android 應用程式周圍建立包裝器。在應用程式換行前，您可以在 Intune 中設定行動 [應用程式管理原則](#)，以變更應用程式的功能。

在執行工具之前，請複查[執行 App Wrapping Tool 的安全性考慮](#)。若要下載工具，請移至 GitHub 上的[Microsoft Intune App Wrapping Tool Android版](#)。

NOTE

如果您有使用 Intune App Wrapping Tool 與您的應用程式有關的問題，請在 GitHub 提交[要求以取得協助](#)。

完成使用 App Wrapping Tool 的必要條件

- 您必須在執行 Windows 7 或更新版本的 Windows 電腦上執行 App Wrapping Tool。
- 您的輸入應用程式必須是副檔名為 apk 的有效 Android 應用程式套件及：
 - 無法加密。
 - 它之前必須尚未由 Intune App Wrapping Tool 所包裝。
 - 必須針對 Android 9.0 或更新版本寫入。

NOTE

如果您的輸入應用程式是 Android 應用程式束 (.aab)，您必須先將其轉換為 APK，才能使用 Intune App Wrapping Tool。如需詳細資訊，請參閱 [轉換 Android 應用程式捆綁 \(AAB\) 至 APK](#)。從2021年8月起，[新的私人應用程式仍可以 APKs 形式發佈到 Google Play 商店](#)。

- 應用程式必須由或為您的公司開發。您無法在 Google Play Store 中提供的應用程式上使用此工具。這包括從 Google Play 商店下載或取得應用程式。
- 若要執行 App Wrapping Tool，您必須安裝最新版的[Java Runtime 環境](#)，然後確定已在您的 Windows 環境變數中將 java 路徑變數設定為 C:\ProgramData\Oracle\JAVA\javapath。如需詳細資訊，請參閱 [JAVA 檔](#)。

NOTE

在某些情況下，32位版本的 JAVA 可能會導致記憶體問題。安裝64位版本是很好的做法。

- Android 需要 () 簽章所有的應用程式套件。如需 [重複使用現有憑證和整體簽署憑證指引](#)，請參閱 [重複使用簽署憑證和包裝應用程式](#)。在您使用 Intune App Wrapping Tool 來包裝 apk 檔案之後，建議使用[Google 的提供 Apksigner 工具](#)。這可確保在您的應用程式取得使用者設備之後，該應用程式可由 Android 標準正確啟動。
- (選用) 有時候，應用程式可能會命中 Dalvik 可執行檔 (DEX) 大小限制，因為在換行時所加入的 Intune MAM SDK 類別。DEX files 是 Android 應用程式編譯的一部分。在換行時，Intune App Wrapping Tool 會

自動處理 DEX 檔案溢出，讓應用程式的最小 API 層級為 21 或以上 () 的 [1.0.2501.1](#)。針對最小 API 層級為 < 21 的應用程式，最佳作法是使用包裝的旗標來增加最小 API 層級 `-UseMinAPILevelForNativeMultiDex`。若客戶無法增加應用程式的最低 API 層級，可使用下列 DEX 溢出的解決方法。在某些組織中，這可能需要使用任何人員編譯 (ie 的應用程式。app 組建小組)：

- 使用 ProGuard 從應用程式的主要 DEX 檔案中去掉未使用的類別參照。
- 針對使用 v 3.1.0 或更高版本 Android Gradle 外掛程式的客戶，請停用 [D8 dexter](#)。

安裝 App Wrapping Tool

1. 從 [GitHub 存放庫](#) 中，將 Intune App Wrapping Tool 的安裝檔 InstallAWT.exe 下載到 Windows 電腦。開啟安裝檔。
2. 接受授權合約，然後完成安裝。

請注意，您已安裝工具的資料夾。預設位置為：C:\Program (x86) \ Microsoft Intune Mobile Application Management\Android\ App Wrapping Tool 的檔案。

執行 App Wrapping Tool

IMPORTANT

Intune 定期發佈 Intune App Wrapping Tool 的更新。定期檢查 [適用於 Android 的 Intune App Wrapping Tool](#) 以進行更新，並併入您的軟體發展發行週期，以確保您的應用程式支援最新的應用程式保護原則設定。

1. 在安裝 App Wrapping Tool 的 Windows 電腦上，開啟 [PowerShell] 視窗。
2. 從安裝工具的資料夾中，匯入 App Wrapping Tool PowerShell 模組：

```
Import-Module .\IntuneAppWrappingTool.psm1
```

3. 使用 AppWrappingTool 命令執行工具，其使用語法如下：

```
Invoke-AppWrappingTool [-InputPath] <String> [-OutputPath] <String> [<CommonParameters>]
```

下表詳述 AppWrappingTool 命令的屬性：

“	“
-InputPath <字串>	來源 Android 應用程式 (的路徑。apk) 。
-OutputPath <字串>	輸出 Android 應用程式的路徑。如果這是與 InputPath 相同的目錄路徑，打包將會失敗。
<CommonParameters>	(選用) 命令支援像是 verbose 和 debug 等通用 PowerShell 參數。

- 如需一般參數的清單，請參閱 [Microsoft Script Center](#)。
- 若要查看工具的詳細使用資訊，請輸入下列命令：

```
Help Invoke-AppWrappingTool
```

範例：

匯入 PowerShell 模組。

```
Import-Module "C:\Program Files (x86)\Microsoft Intune Mobile Application Management\Android\App Wrapping Tool\IntuneAppWrappingTool.psm1"
```

在原生應用程式上執行 App Wrapping Tool HelloWorld apk。

```
invoke-AppWrappingTool -InputPath .\app\HelloWorld.apk -OutputPath .\app_wrapped\HelloWorld_wrapped.apk - Verbose
```

會產生換行應用程式及記錄檔，並儲存在您指定的輸出路徑中。

我應該多久使用 Intune App Wrapping Tool 來 rewrap 我的 Android 應用程式？

您需要 rewrap 應用程式的主要案例如下：

- 應用程式本身已發行新版本。舊版本的應用程式被包裝並上傳至 Intune 主控台。
- 適用於 Android 的 Intune App Wrapping Tool 已發行新版本，可啟用主要錯誤修正，或全新的 intune 應用程式保護原則功能。這會在每6-8 星期的 GitHub Microsoft Intune 的 [App Wrapping Tool 為 Android](#) 的儲存機制。

Rewrapping 的一些最佳作法包括：

- 維護在建立程式期間使用的簽署憑證，請參閱 [重複使用簽署憑證和包裝應用程式](#)

重複使用簽署憑證及換行應用程式

Android 要求所有應用程式必須由有效的憑證簽署，才能安裝在 Android 裝置上。

在使用現有的簽章工具進行包裝 後，可以使用現有的簽章工具簽署應用程式。() 會在換行之前，先將應用程式中的 如果可能的話，在換行期間，應使用建立過程中已使用的簽署資訊。在某些組織中，這可能需要使用誰擁有金鑰庫資訊 (ie。app 組建小組) 。

如果無法使用前一個簽署憑證，或應用程式尚未部署，您可以遵循 [Android 開發人員指南](#) 中的指示，建立新的簽署憑證。

若應用程式以前已使用不同的簽署憑證進行部署，則在升級後無法將應用程式上傳至 Intune。如果您的應用程式簽署的憑證與應用程式建立的憑證不同，將會中斷應用程式升級案例。因此，應維護所有新的簽署憑證，以進行應用程式升級。

執行 App Wrapping Tool 的安全性考慮

若要防止可能的欺騙性、資訊披露和權限提高攻擊：

- 確定公司的輸入營運 (LOB) 應用程式，以及輸出應用程式位於 App Wrapping Tool 執行所在的 Windows 電腦上。
- 在執行工具的相同機器上，將輸出應用程式匯入到 Intune。如需 JAVA keytool 的詳細資訊，請參閱 [keytool](#) 。
- 如果輸出應用程式和工具位於通用命名慣例 (UNC) 路徑，而且您未在同一部電腦上執行工具和輸入檔案，請使用 [網際網路通訊協定安全性 \(IPsec\)](#) 或 [伺服器消息區塊 \(SMB\) 簽署](#)，將環境設定為安全。

- 確定應用程式來自于受信任的來源。
- 保護具有包裝應用程式的輸出目錄。請考慮使用使用者層級目錄來輸出。

將 Android 應用程式束 (AAB) 轉換為 APK

Intune App Wrapping Tool 目前只支援 APK 輸入。Android 應用程式束必須先轉換成 APK, 以與工具搭配使用。

您可以使用[Google 的命令列工具](#), `bundletool` 將 Android 應用程式捆綁包轉換為 APK。最新版本的 `bundle-tool` 可從 Google 的[bundletool GitHub](#)儲存機制中下載。

`bundletool` 可用於產生單一通用 APK 以搭配 Intune App Wrapping Tool 使用下列命令：

```
bundletool build-apks --bundle=input.aab --mode=universal --output=input.apks
```

`.apks` 輸出檔是包含單一通用 APK 檔案的 ZIP 封存。解壓縮封存, 並使用該 APK 檔案作為 Intune App Wrapping Tool 的輸入。

另請參閱

- [決定如何使用 Microsoft Intune 為行動應用程式管理準備應用程式](#)
- [適用於 Android 開發人員指南的 Microsoft Intune 應用程式 SDK](#)

Microsoft Intune 應用程式 SDK Xamarin 系結

2022/9/27 •

NOTE

您可以先閱讀[Intune 應用程式 SDK](#)文章的入門，它會說明如何準備在每個支援的平臺上進行整合。

概觀

[Intune 應用程式 SDK Xamarin](#)系結可在使用 Xamarin 建立的 iOS 和 Android 應用程式中啟用[Intune 應用程式保護原則](#)。系結可讓開發人員在 Intune 應用程式保護功能中輕鬆地建立在其 Xamarin 型應用程式中。

Microsoft Intune 應用程式 SDK Xamarin 系結可讓您將 Intune 應用程式保護原則，(也稱為應用程式或 MAM 原則，) 到以 Xamarin 開發的應用程式中。具有 MAM 功能的應用程式是與 Intune 應用程式 SDK 整合的應用程式。當 Intune 主動管理應用程式時，IT 管理員可以將應用程式保護原則部署至行動應用程式。

受支援的功能為何？

開發人員電腦

- Windows (Visual Studio 版本 15.7 +)
- macOS

行動應用程式平臺

- Android
- iOS

Intune 行動應用程式管理案例

- Intune [MAM](#)
- Intune MDM 註冊裝置
- 協力廠商的 EMM 註冊裝置

使用 Intune 應用程式 SDK Xamarin 系結的 Xamarin 應用程式，現在可以在 Intune 行動裝置管理 (MDM) 註冊裝置和 unenrolled 裝置上接收 Intune 應用程式保護原則。

必要條件

查看 [授權條款](#)。列印並保留您記錄的授權條款複本。下載並使用 Intune 應用程式 SDK Xamarin 系結，即表示您同意這類授權條款。如果您未接受，請勿使用軟體。

Intune SDK 依賴[Microsoft 驗證程式庫來 \(MSAL\)](#) 針對其[驗證](#)及條件式啟動案例，這需要以[Azure Active Directory](#)設定應用程式。

如果您的應用程式已設定為使用 MSAL，且有其自己的自訂用戶端識別碼，用以對 Azure Active Directory 進行驗證，請務必遵循下列步驟，將您的 Xamarin 應用程式的許可權授與 Intune Mobile 應用程式管理 (MAM) 服務。請使用[INTUNE SDK 指南快速入門](#)中的「[將您的應用程式授與 intune app protection service 的存取權](#)」一節中的指示。

安全性考量

若要防止可能的欺騙性、資訊披露和權限提高攻擊：

- 確定在安全的工作站上進行 Xamarin 應用程式開發。
- 確定系統來自有效的 Microsoft 來源：
 - [MS Intune 應用程式 SDK NuGet 設定檔](#)
 - [Intune 應用程式 SDK Xamarin GitHub 存放庫](#)
- 為專案設定 NuGet 的 config，以信任已簽署、未修改的 NuGet 套件。如需詳細資訊，請參閱 [安裝已簽署的套件](#)。
- 保護包含 Xamarin 應用程式的輸出目錄。請考慮使用使用者層級目錄來輸出。

在您的 iOS 行動裝置應用程式中啟用 Intune 應用程式保護原則

IMPORTANT

Intune 定期發佈 Intune 應用程式 SDK 的更新。請定期檢查 [Intune 應用程式 SDK Xamarin](#) 系結以取得更新，並併入您的軟體發展發行週期，以確保您的應用程式支援最新的應用程式保護原則設定。

1. 將 [iOS NuGet 套件](#) 新增至您的 Xamarin iOS 專案。
2. 遵循將 Intune 應用程式 SDK 整合至 iOS 行動裝置應用程式所需的一般步驟。您可以從 Intune 應用程式 SDK 的整合指示中的步驟3開始，以 [iOS 開發人員指南](#)。您可以略過該區段中執行 IntuneMAMConfigurator 的最後一個步驟，因為此工具組含在套件 iOS 中，且會在建立時自動執行。重要事項：在從 Xcode 的 Visual Studio 中啟用應用程式的金鑰鏈共用稍有不同。開啟應用程式的權利 plist，確定已啟用「啟用金鑰鏈」選項，且該區段中新增了適當的金鑰鏈共用群組。然後，確定所有適當設定/平臺組合之專案之「iOS 系出簽署」選項的「自訂權利」欄位中指定的權利 plist。
3. 在新增系結並正確設定應用程式之後，您的應用程式便可以開始使用 Intune SDK 的 APIs。若要這麼做，您必須包含下列命名空間：

```
using Microsoft.Intune.MAM;
```

4. 若要開始接收應用程式保護原則，您的應用程式必須在 Intune MAM 服務中註冊。如果您的應用程式未使用 [Microsoft 驗證程式庫](#) (MSAL) 來驗證使用者，而您想要 Intune SDK 處理驗證，您的應用程式應將使用者的 UPN 提供給 IntuneMAMEnrollmentManager 的 LoginAndEnrollAccount 方法：

```
IntuneMAMEnrollmentManager.Instance.LoginAndEnrollAccount([NullAllowed] string identity);
```

如果使用者的 UPN 在通話時是未知的，則應用程式可能會傳入 null。在此情況下，系統會提示使用者輸入他們的電子郵件地址和密碼。

如果您的應用程式已使用 MSAL 來驗證使用者，您可以在您的應用程式與 Intune SDK 之間設定單一登入 (SSO) 體驗。首先，您必須覆寫 Intune SDK 所使用的預設 AAD 設定與您的應用程式。您可以透過 IntuneMAMSettings 字典在應用程式的 Info 中做到這一點，如在 [iOS 開發人員指南](#) 中的 [Intune 應用程式 SDK](#) 中所述，您也可以透過 plist 的 IntuneMAMSettings 類別的屬性覆寫，在程式 AAD 代碼中這麼做。建議使用 plist 方法，以供 MSAL 設定為靜態的應用程式使用時，建議將覆寫屬性設定為靜態的應用程式，以便在執行時間決定這些值的應用程式。在設定所有 SSO 設定後，您的應用程式應該在驗證成功之後，將使用者的 UPN 提供給 IntuneMAMEnrollmentManager 的 RegisterAndEnrollAccount 方法：

```
IntuneMAMEnrollmentManager.Instance.RegisterAndEnrollAccount(string identity);
```

應用程式可以在 IntuneMAMEnrollmentDelegate 的子類中執行 EnrollmentRequestWithStatus 方法，並將 IntuneMAMEnrollmentManager 的委派屬性設定為該類別的實例，以判斷註冊嘗試的結果。

順利註冊後，如果您查詢下列屬性，則應用程式可以決定已註冊帳戶 (的 UPN (如果先前是未知))：

```
string enrolledAccount = IntuneMAMEnrollmentManager.Instance.EnrolledAccount;
```

範例應用程式

範例應用程式會反白顯示 Xamarin 中的 MAM 功能。iOS 的應用程式可在[GitHub](#)上使用。

NOTE

iOS/iPadOS 沒有 remapper。整合至 Xamarin.Forms 應用程式應該與一般 Xamarin iOS 專案相同。

在您的 Android 行動裝置應用程式中啟用 Intune 應用程式保護原則

1. 將 web.config [NuGet 封裝](#)新增至您的 Xamarin android 專案。
 - a. 若為 Xamarin.Forms 應用程式，請將[Remapper NuGet 套件的套裝軟體](#)新增至您的 Xamarin 專案。
2. 請遵循將 [Intune 應用程式 SDK 整合](#) 至 Android 行動裝置應用程式所需的一般步驟，請參閱本檔以取得其他詳細資料。

Xamarin 和 Android 整合

有關整合 Intune 應用程式 SDK 的完整概述，可在《[Microsoft Intune 應用程式 sdk for Android 開發人員指南](#)》中找到。當您通讀指南並整合 Intune 應用程式 SDK 與 Xamarin 應用程式時，下列各節旨在強調在 JAVA 中開發的原生 Android 應用程式和以 c# 開發之 Xamarin 應用程式的實現之間的差異。這些區段應視為補充性，無法取代完整閱讀指南。

Remapper

從 1.4428.1 版本開始，`Microsoft.Intune.MAM.Remapper` 套件可以新增至 Xamarin 應用程式，做為 [組建工具](#)，以執行 MAM 類別、方法和系統服務取代。如果包含 Remapper，則會在建立應用程式時，自動執行已重新命名的方法和 MAM 應用程式區段的 MAM 對等取代部分。

若要從 ification 由 Remapper 排除類別，您可以在專案 `.csproj` 檔案中新增下列屬性。

```
<PropertyGroup>
  <ExcludeClasses>Semicolon separated list of relative class paths to exclude from MAM-
  ification</ExcludeClasses>
</PropertyGroup>
```

NOTE

Remapper 目前禁止在 Android 應用程式中進行調試。建議使用手動整合，以調試應用程式。

重新命名的方法

在許多情況下，Android 類別中的可用方法在 MAM 取代類別中已標示為終稿。在此情況下，MAM 取代類別會提供類似命名的方法，(尾碼為您應改為使用 `MAM`) 尾碼。例如，從 `MAMActivity` 派生，而不是覆寫 `OnCreate()` 及呼叫 `base.OnCreate()`，`Activity` 必須覆寫 `OnMAMCreate()` 及呼叫 `base.OnMAMCreate()`。

MAM 應用程式

您的應用程式必須定義 `Android.App.Application` 類別。若要手動整合 MAM，它必須從 `MAMApplication` 繼承。請確定您的子類已使用 `[Application]` 屬性適當地修飾，並覆寫 `(IntPtr, JniHandleOwnership)` 建構函式。

```
[Application]
class TaskrApp : MAMApplication
{
    public TaskrApp(IntPtr handle, JniHandleOwnership transfer)
        : base(handle, transfer) { }
```

NOTE

使用 MAM Xamarin 系統時，可能會導致應用程式當以偵錯模式部署時即損毀。在此情況下，必須將屬性加入

`Application` 類別中，而且 `android:debuggable="true"` 必須從資訊清單中移除旗標（如果手動設定）
`Debuggable=false` 。

啟用需要參與應用程式的功能

範例:判斷應用程式是否需要 PIN 碼

```
MAMPolicyManager.GetPolicy(currentActivity).IsPinRequired;
```

範例:判斷主要 Intune 使用者

```
IMAMUserInfo info = MAMComponents.Get<IMAMUserInfo>();
return info?.PrimaryUser;
```

範例:判斷是否允許儲存至裝置或雲端儲存體

```
MAMPolicyManager.GetPolicy(currentActivity).GetIsSaveToLocationAllowed(SaveLocation service, String
username);
```

從 SDK 註冊通知

您的應用程式必須透過建立 `MAMNotificationReceiver` 及註冊 `MAMNotificationReceiverRegistry`，向 SDK 註冊通知。如下列範例所示，您可以透過提供接收器及所需的通知類型來完成這項 `App.OnMAMCreate` 作業：

```
public override void OnMAMCreate()
{
    // Register the notification receivers
    IMAMNotificationReceiverRegistry registry = MAMComponents.Get<IMAMNotificationReceiverRegistry>();
    foreach (MAMNotificationType notification in MAMNotificationType.Values())
    {
        registry.RegisterReceiver(new ToastNotificationReceiver(this), notification);
    }
    ...
}
```

MAM 註冊管理員

```
IMAMEnrollmentManager mgr = MAMComponents.Get<IMAMEnrollmentManager>();
```

Xamarin.Forms 整合

針對應用程式，`Microsoft.Intune.MAM.Remapper` 該包會將類別插入常用 `Xamarin.Forms` 類別的類別階層中，以 `Xamarin.Forms` 自動 `MAM` 執行 MAM 類別的取代。

NOTE

除了上述所述之 Xamarin 整合之外，也必須執行 Xamarin.Forms 整合。Remapper 應用程式的行為會與 Xamarin.Forms 不同，所以手動 MAM 取代仍然必須執行。

將 Remapper 新增至您的專案後，您將需要執行 MAM 對等取代。例如，`FormsAppCompatActivity` 您可以繼續在應用程式中使用它 `FormsApplicationActivity` 所提供的覆寫 `OnResume` `OnCreate`，而且會以 MAM `OnMAMCreate` 對等 `OnMAMResume` 專案取代。

```
public class MainActivity : global::Xamarin.Forms.Platform.Android.FormsAppCompatActivity
{
    protected override void OnMAMCreate(Bundle savedInstanceState)
    {
        base.OnMAMCreate(savedInstanceState);
        global::Xamarin.Forms.Forms.Init(this, savedInstanceState);
        LoadApplication(new App());
    }
}
```

若未進行取代，則在進行取代之前，您可能會遇到下列編譯錯誤：

- **編譯器錯誤 CS0239**。此為此表單

```
'MainActivity.OnCreate(Bundle)': cannot override inherited member
'MAMAppCompatActivityBase.OnCreate(Bundle)' because it is sealed
```

中通常會出現此錯誤。這是預期的，因為當 Remapper 修改 Xamarin 類別的繼承時，會進行 `sealed` 某些功能，並將新的 MAM variant 新增至覆寫。

- **編譯器錯誤 CS0507**：此表單

```
'MyActivity.OnRequestPermissionsResult()' cannot change access modifiers when overriding 'public'
inherited member ...
```

中常見會出現此錯誤。當 Remapper 變更某些 Xamarin 類別的繼承時，某些成員函數會變更為 `public`。如果您覆寫這些函數中的任何一種，您也需要變更這些功能的存取修飾符 `public`。

NOTE

Remapper 會重新撰寫 Visual Studio 用於 IntelliSense 自動完成的相依性。因此，當為 IntelliSense 新增 Remapper 時，您可能需要重新載入並重建專案，才能正確辨識變更。

正在疑難排解

- 如果您在啟動的應用程式中遇到空白的白色畫面，您可能需要強制對主執行緒執行導覽呼叫。
- 由於 MvvmCross 與 Intune MAM 類別之間的衝突，Intune SDK Xamarin 系統不支援使用跨平臺架構（如 MvvmCross）的應用程式。雖然某些客戶在將其應用程式移至純 Xamarin.Forms 後可能會成功整合，但我們並未為使用 MvvmCross 的應用程式開發人員提供明確的指引或外掛程式。

公司入口網站應用程式

Intune SDK Xamarin 系統依賴裝置上的[公司入口網站](#)Android 應用程式是否存在，才能啟用應用程式保護原則。公司入口網站會從 Intune 服務中檢索應用程式保護原則。當應用程式初始化時，它會載入原則及程式碼，以從公司入口網站強制執行該原則。使用者不需要登入。

NOTE

當 Android 裝置上沒有公司入口網站應用程式時，Intune 管理的應用程式的行為與不支援 Intune 應用程式保護原則的一般應用程式相同。

針對不含裝置註冊的應用程式保護，使用者 **不** 需要使用公司入口網站 app 註冊裝置。

範例應用程式

範例應用程式在[GitHub](#)上提供了 Xamarin 和 Xamarin.Forms 應用程式中的 MAM 功能。

支援

如果您的組織是現有的 Intune 客戶，請與您的 Microsoft 支援代表合作，以開啟支援票證，並在 [\[GitHub 問題\] 頁面上](#) 建立問題。我們將協助您儘快進行協助。